LAB2 Digital Certificates

Monica Tamanampudi
P.no.960207-4180
Email:mota17@student.bth.se

Task 1: [v3_ca]

Subject Key Identifier: The subject key identifier extension provides a means of identifying
certificates that contain a public key.
Basic constraints: 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 name followed by a non-negative value can be included.
The OpenSSL config file has CA:true.
Key Usage: Key usage is a multi-valued extension consisting of a list of names of the permitted key usages.
The supported names are: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly and decipherOnly.
The digitalSignature bit is asserted 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 asserted when the subject public key is used for verifying signatures on certificate revocation lists (e.g., CRLs, delta CRLs, or ARLs).
The keyCertSign bit is asserted when the subject public key is used for verifying signatures on public key certificates. If the keyCertSign bit is asserted, then the CA bit in the basic constraints extension (Section 4.2.1.9) MUST also be asserted.
The OpenSSL config file has critical, digitalSignature,cRLSign, keyCertSign.
Authority Key Identifier: The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. This extension is used where an issuer has multiple signing keys (either due to multiple concurrent key pairs or due to changeover). The identification MAY be based on either the key identifier (the subject key identifier in the issuer's certificate) or the issuer name and serial number.
The OpenSSL config file has keyid: always, issuer.
Netscape String extensions: Netscape Comment (nsComment) is a string extension containing a comment which will be displayed when the certificate is viewed in some browsers.
Netscape Certificate Type

This is a multi-valued extension which consists of a list of flags to be included. It was used to indicate the purposes for which a certificate could be used. The basicConstraints, keyUsage and extended key usage extensions are now used instead.
Acceptable values for nsCertType are: client, server, email, objsign, reserved, sslCA, emailCA, objCA .

Task 2: [v3_intermediate_ca]

subjectKeyIdentifier = hash
The subject key identifier extension provides a means of identifying certificates that contain a public key.
authorityKeyIdentifier = keyid:always,issuer
The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.
basicConstraints = critical, CA:true, pathlen:0
critical indicates the extensions are critical.
CA:true indicates that a certificate is a CA certificate.
Pathlen of 0 indicates that it can be used to sign end user certificates only. This is the Difference between the v3_ca and v3_intermediate_ca. So v3_ca, can have certificates below the chain.

Task 3: [usr_cert]

The Basic constraints CA:False indicate that this is not a CA certificate.
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
critical – the extension will be critical.
nonrepudiation - bit is asserted 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.
keyEncipherment - bit is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.
The digitalSignature bit is asserted 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.

"OpenSSL Generated Certificate" - This will be displayed in Netscape's comment listbox.
subjectKeyIdentifier=hash
The subject key identifier extension provides a means of identifying certificates that contain a public key.
authorityKeyIdentifier=keyid,issuer
The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.

Task 4: [server_cert]

The Basic constraints CA:False indicate that this is not a CA certificate.
keyUsage = critical, digitalSignature, keyEncipherment
critical – the extension will be critical.
keyEncipherment - bit is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.
The digitalSignature bit is asserted 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.
subjectKeyIdentifier=hash
The subject key identifier extension provides a means of identifying certificates that contain a public key.
authorityKeyIdentifier=keyid,issuer
The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate.
extendedKeyUsage = serverAuth
serverAuth indicates SSL/TLS Web Server Authentication.

Task 5: [Policies]

In the "policy_match" policy, all fields listed as "match" must contain the exact same contents as that field in the CA's DN. All fields listed as "supplied" must be present. All fields listed as "optional" are allowed, but not required to be there. Anything allowed must be listed! So, this policy requires the same country, State, and Organization name as the CA for all certs it signs.
"policy_anything" policy is where the certificate will accept anything, and only require a CN.

Task 6: Options for the root certificate

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

The private key in private/root.key.pem is read in command line.

-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.

7300 days is specified in command line.

-[digest]: this specifies the message digest to sign the request with (such as -md5, -sha1). This overrides the digest algorithm specified in the configuration file.

-sha256: is the message digest used to sign the request.

-extensions section: these options specify 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.

V3_ca section is specified in command line.

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

The Output is written to the file certs/root.cert.pem

Task 7: Verify the root certificate

```
openssl x509 -noout -text -in certs/root.cert.pem
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 10223778126063265383 (0x8de22809aa68e667)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica Root
```

```
Validity
Not Before: Jan 17 20:46:06 2018 GMT
Not After : Jan 12 20:46:06 2038 GMT
Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica Root
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (4096 bit)
Modulus:
00:c4:28:03:12:21:c4:b5:55:6a:bc:43:a4:1e:82:
34:a1:00:e5:ad:55:c2:0d:92:df:f4:e2:68:e0:46:
02:73:ad:e7:17:ab:f1:4e:86:cd:50:7e:89:be:92:
76:bc:b2:90:ca:17:7f:37:df:0a:c6:b0:f1:46:e1:
dc:af:a4:eb:38:0b:f7:59:f3:7b:d0:c5:aa:94:c0:
e0:08:c6:02:7d:cb:26:07:eb:b0:58:eb:00:4a:88:
73:bd:da:7f:37:28:88:36:fb:09:31:21:3c:0a:92:
3f:e7:af:91:f8:b1:aa:86:85:41:d4:c4:48:6d:5e:
4c:b2:6c:34:db:cf:42:11:aa:a1:e5:6d:46:37:d4:
0d:31:0b:0c:20:51:83:23:d0:8e:d6:0a:01:c3:ec:
27:bc:c0:fc:ed:9d:4f:14:c1:57:0b:47:eb:ee:81:
2d:4c:71:b3:4d:94:00:0e:cd:c0:34:71:69:b0:17:
62:8a:22:d3:70:bd:9c:fa:b4:31:81:8a:7e:85:c5:
af:a9:81:ad:4a:6c:eb:47:73:a1:9a:ae:af:a4:5b:
81:72:43:ef:f1:f1:c5:d1:c6:e7:84:b8:ee:07:4c:
0e:fa:01:ae:9a:aa:63:dc:7f:10:fc:1b:26:07:6b:
17:a5:b5:c6:68:84:94:d5:14:b2:fa:4a:2f:b4:ba:
07:c6:41:32:d2:7f:aa:d9:1c:5d:97:b9:af:dc:b1:
a8:71:1f:cf:63:18:ea:69:0f:b2:34:0a:09:99:54:
34:d1:cb:48:87:e5:f7:e5:5c:2c:c6:e7:38:9f:b7:
b9:c1:88:d2:60:2d:13:5c:c4:59:c4:ef:b6:37:c1:
87:90:84:f1:21:3f:78:8c:37:dc:35:4d:34:49:0a:
2c:13:0f:54:60:2e:25:39:0b:40:d0:32:ce:5a:7b:
7e:33:ea:10:d6:7f:7b:62:ff:78:ce:0c:9f:ca:c7:
a6:50:64:a2:71:46:c5:28:06:2c:97:92:a0:a5:cd:
06:d5:50:2d:49:a5:32:e2:26:49:d0:57:b9:11:b7:
f3:e9:70:72:11:ae:21:3a:f3:39:ba:f1:35:6f:da:
cf:28:05:86:21:2a:c8:11:18:6c:25:b4:14:44:1a:
57:fd:4d:99:7b:cd:45:e6:bc:4c:71:01:3a:4d:96:
```

```
0a:f1:9f:4d:20:d8:0e:8a:69:df:9f:cd:2a:d0:30:
a3:4e:1e:43:b9:32:f9:18:cb:40:98:1f:4b:f6:0a:
c1:af:b7:ed:06:57:99:e4:ae:77:15:bc:84:ac:c1:
c9:d7:ec:f1:f3:05:5b:46:59:27:c8:fe:36:b1:67:
7f:1a:96:c1:d4:92:0e:af:d7:ce:fb:d1:eb:88:0b:
9b:e7:cb
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
33:0B:E1:67:75:A9:06:A5:4E:2B:52:B1:9F:37:26:79:66:B7:7E:76
X509v3 Authority Key Identifier:
keyid:33:0B:E1:67:75:A9:06:A5:4E:2B:52:B1:9F:37:26:79:66:B7:7E:76

X509v3 Basic Constraints:
CA:TRUE
X509v3 Key Usage: critical
Digital Signature, Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
2e:c0:28:ef:d3:8d:91:b5:8e:8d:83:33:02:02:a1:e0:0f:f4:
6a:dc:af:28:91:0c:cc:d4:a1:52:f9:69:b9:97:f2:ee:3f:94:
08:1c:4c:4b:9b:c6:95:b3:5b:07:08:ba:30:75:c9:47:3c:b4:
c0:c0:6e:5c:0d:4b:f9:75:53:34:c9:b8:e3:3a:09:5e:cd:b0:
58:41:3d:15:ee:15:8d:46:a1:1a:55:e3:66:f8:b7:32:8c:fa:
9a:38:4f:3e:1f:ec:ba:c2:0c:5b:43:f1:01:53:cc:16:0b:65:
4b:c4:0b:c1:2a:85:6a:93:d2:8f:74:ae:c4:3f:90:32:e5:4f:
2e:48:ed:d4:3f:24:14:a4:ef:d9:19:87:7a:3c:29:1e:c4:a2:
2a:21:f4:47:4f:b7:89:2c:72:49:4c:ce:cf:95:23:eb:1b:7d:
0c:50:bd:2c:52:a3:93:6b:3d:18:e4:d7:a2:45:6b:0b:0e:07:
13:3d:16:04:15:de:cc:4a:44:02:56:a6:9b:49:fe:7f:bd:ae:
a5:3f:73:77:1f:bf:f1:41:cd:dc:c4:f2:e9:09:4e:c6:07:50:
43:58:aa:d0:e6:02:95:ac:cc:91:22:11:f2:cd:0c:95:f3:44:
7b:dc:91:dc:b6:04:57:5c:4e:95:6c:5c:67:70:8c:0a:7f:76:
ed:4f:c9:f5:26:fc:b4:18:0b:ec:06:91:00:bd:7e:1c:f0:1f:
46:19:6f:f2:3a:9e:eb:5f:30:b5:da:95:db:54:df:98:b7:de:
a0:29:a1:19:0c:e0:f2:16:fe:75:c2:a9:7b:05:6b:5d:93:18:
bf:b3:32:97:f4:e8:94:7f:64:2d:85:fe:f0:da:db:c4:33:55:
47:05:b7:2d:80:57:7d:ee:e0:11:9f:21:38:d1:6c:b3:02:19:
```

```
aa:71:5c:e5:90:19:e7:85:67:ca:b7:c5:1f:95:fa:5f:d6:9d:
c9:ab:3b:02:49:f4:5c:4c:d7:ce:b0:77:a5:b1:44:73:61:cd:
75:a0:9a:a4:11:53:bc:30:89:9b:55:8b:a9:6f:db:cc:3a:00:
54:a3:bd:0c:7d:33:f8:9f:2b:e9:7e:58:bc:24:8a:0d:ad:89:
4b:d3:34:da:a1:3b:f8:37:3e:48:8b:92:6a:d9:8f:4d:e1:fa:
84:9f:73:f3:2e:a8:ad:5c:1e:a9:98:d2:72:f8:74:7a:b3:db:
3b:ab:13:e9:c5:15:09:34:86:90:1f:cf:02:cf:74:7e:b1:b0:
ec:05:3c:75:36:4e:7e:1a:8a:8f:5d:76:3c:7c:ee:39:36:ad:
b2:db:66:8c:47:18:01:d6:b4:de:cc:db:ac:98:96:9d:9d:e2:
11:19:47:87:e8:8d:d6:0d
```

```
openssl req -config ca1/openssl.cnf -new -sha256 -key ca1/private/ca1.key.pem -
out ca1/csr/ca1.csr.pem
Enter pass phrase for ca1/private/ca1.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 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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:monica CA1
Email Address []:

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

Task 8: Verify the CSR

```
            openssl req -text -noout -verify -in ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica CA1
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
        Modulus:
          00:b5:49:0c:1a:29:58:df:cf:c5:0c:44:1a:74:b5:
          ff:3e:01:83:c8:ae:51:5f:23:97:40:4c:d5:ee:42:
          2d:0d:76:2a:e1:d1:8f:96:fe:af:05:13:2b:eb:08:
          b1:08:0f:34:1b:7b:e8:7f:99:e8:6d:e1:2c:ec:71:
          2f:bb:70:00:26:aa:62:5b:cb:c4:f4:bd:ef:da:20:
          68:18:a8:16:31:5f:e1:10:88:0e:5e:7e:ea:6a:80:
          92:ee:d6:e5:ea:b5:fa:46:5e:9b:55:55:47:05:c9:
          65:68:a6:9e:42:de:fb:0b:e2:c2:01:db:68:b3:44:
          39:c7:d8:ef:35:6e:0a:d4:8b:a4:a9:0f:12:37:3b:
          d3:6e:e0:8e:e9:9b:4c:96:b8:fb:f2:42:49:dc:19:
          6e:2f:45:d7:3f:ae:3e:f0:4d:e3:3d:e2:94:81:36:
          e4:7a:e9:cf:a7:2c:6d:e1:13:8b:22:72:4a:d2:93:
          58:fb:09:4f:76:ec:ff:87:21:c3:f5:3c:fc:55:40:
          fe:8c:eb:a5:f8:54:28:5c:58:35:fc:4f:57:20:97:
          7e:42:86:05:1d:ad:ff:5c:1f:ab:80:71:8c:7f:ab:
          8b:0a:3f:c9:46:50:50:e8:eb:50:74:95:35:e8:61:
          a8:20:9f:e8:ac:ed:8d:c4:08:03:d5:40:68:ea:db:
          89:db:73:17:be:a7:f0:64:63:4a:22:3e:3d:39:3d:
          07:ae:86:27:b4:ea:db:43:49:da:4e:db:64:c1:5e:
          97:81:fb:2d:98:88:f8:ff:df:ba:4f:ef:b7:76:65:
          3a:a5:26:99:c4:7d:cb:2f:2b:2e:50:fc:e2:21:a6:
          12:f7:51:5b:90:d1:0c:35:f1:20:61:b9:c2:35:b1:
          48:66:e0:18:75:78:d2:04:4e:2f:e1:12:d8:e2:57:
          28:d9:00:22:74:60:3f:35:cc:1f:e9:b3:53:08:45:
```

```
                    da:25:bd:21:03:a0:bb:cd:58:f7:20:f3:ec:07:6a:
                    0b:07:e0:64:48:ae:52:61:6a:87:dd:07:09:b2:05:
                    0e:81:f7:8e:de:0b:58:01:88:07:64:2e:34:0d:d4:
                    19:88:be:df:bf:94:0a:6b:3c:a3:96:fd:d0:c9:ae:
                    85:79:11:80:5e:ce:7e:d2:95:ba:01:62:06:88:07:
                    13:13:d0:ff:da:73:23:e3:f4:80:db:0b:51:50:43:
                    6a:41:45:8c:5d:ee:d2:ad:14:0c:1b:3d:93:4c:1f:
                    4d:9c:0c:93:12:99:ce:90:f0:a8:92:bd:1e:93:00:
                    0a:1f:3f:6e:66:8c:ab:3f:e4:56:5c:04:60:2a:b0:
                    6f:48:7b:86:c2:03:2a:82:4d:72:3b:01:2c:80:9e:
                    70:e8:8d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         1d:cc:c2:70:06:a2:d2:d3:67:df:27:ca:62:6f:64:3b:3b:59:
         b5:11:58:2c:26:ab:3b:b8:aa:f4:dc:99:3e:c3:72:35:dc:33:
         e1:bf:e4:aa:2e:07:de:8b:f5:ef:ed:bd:c9:d3:3e:30:ec:5a:
         5a:82:94:27:58:a7:4e:d7:b8:12:45:c1:72:8e:a3:a9:41:c5:
         16:c8:6f:bd:e1:07:72:d4:96:35:14:86:ab:28:5a:65:a9:05:
         9c:4b:c4:91:a9:08:df:f8:b9:f6:f9:62:c6:d4:17:d9:9a:ca:
         34:5c:bf:f9:f0:22:c1:9a:6c:93:4b:de:1b:f1:ff:2b:92:61:
         3d:ba:d6:c5:1c:df:4b:f1:7e:5c:80:9c:7c:2a:55:c3:30:82:
         4f:f0:da:b0:50:b6:21:d3:7d:61:48:ed:f3:58:0f:e3:e4:72:
         47:71:a9:95:2b:d9:23:bc:bf:51:8a:42:dc:13:81:58:83:3b:
         0b:35:6a:c2:90:a8:e1:2b:f9:78:4f:63:ad:19:c7:4e:7d:9e:
         ac:fa:6d:a1:f1:fb:23:77:fd:af:9f:2b:dd:28:a1:a7:f8:fe:
         90:c2:d4:4d:38:89:a9:1d:65:63:ac:ad:8d:71:61:f4:2d:5d:
         ac:6e:da:25:93:a6:3f:1b:ec:20:56:d7:82:9c:1b:e0:fd:cd:
         f5:d5:87:f4:cb:1b:74:f4:00:ca:57:79:d5:42:76:e2:72:31:
         6c:c0:88:83:d3:0d:c7:20:1c:32:f3:4b:9d:43:b6:84:f4:99:
         8a:4e:1b:44:bc:7b:90:b8:04:9e:8c:d8:f4:43:43:d8:d0:20:
         bd:f4:a8:92:7f:ed:3c:13:13:2e:c5:81:c9:f8:39:d7:0e:44:
         91:fc:b4:40:34:c7:a7:de:d8:ef:5f:e0:df:6a:2f:db:f4:1d:
         65:0e:64:98:11:0f:db:82:52:79:ba:8d:27:90:6e:3d:e5:78:
         c8:27:19:ca:59:27:1d:8b:c7:9c:79:0e:06:e9:2d:65:6f:b5:
         6e:7a:57:c1:cd:89:45:88:08:49:bb:68:38:a4:f2:cf:f9:ff:
```

```
         e8:f8:49:4b:08:62:01:4a:55:25:50:ec:b5:aa:1b:c5:3b:52:
         e4:6a:11:43:70:76:4f:45:c7:3e:32:45:1c:45:94:3d:1d:70:
         47:52:ca:13:ff:31:d5:5f:87:47:ff:e9:48:27:c2:ad:1a:0a:
         e2:02:88:ce:30:00:d7:09:6b:90:89:d1:2b:bc:f0:f7:3e:92:
         75:39:b5:38:d1:5d:72:d6:8c:0b:48:f1:9a:c9:d1:d7:8d:8e:
         43:00:76:9b:8a:1a:4d:9e:4f:5a:ed:a9:52:ff:5d:03:9f:fb:
         7a:12:99:7f:ac:fe:08:47
```

```
 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/ats/mota17_ca/private/root.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
                                             Validity
            Not Before: Jan 17 21:05:13 2018 GMT
            Not After : Jan 15 21:05:13 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            organizationName          = ET2540
            commonName                = monica CA1
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16
            X509v3 Authority Key Identifier:
                keyid:33:0B:E1:67:75:A9:06:A5:4E:2B:52:B1:9F:37:26:79:66:B7:7E:76

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Jan 15 21:05:13 2028 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
Data Base Updated
```

Task 9: Options for intermediate CA certificate

-config filename: specifies the configuration file to use.
-notext: don't output the text form of a certificate to the output file.
-days arg: the number of days to certify the certificate for.
3650 days is given as arg in command line.
-md alg: the message digest to use. Possible values include md5, sha1 and mdc2. This option also applies to CRLs.
Sha256 is used as the message digest.
-in filename: an input filename containing a single certificate request to be signed by the CA.
ca1/csr/ca1.csr.pem is the input file.
-out filename: 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.
ca1/certs/ca1.cert.pem is the output file.
-extensions section: 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. See the:w x509v3_config(5) manual page for details of the extension section format.

Task 10: Verify the certificate for CA1

```
ats@serverA:~/mota17_ca$ 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=monica Root
    Validity
```

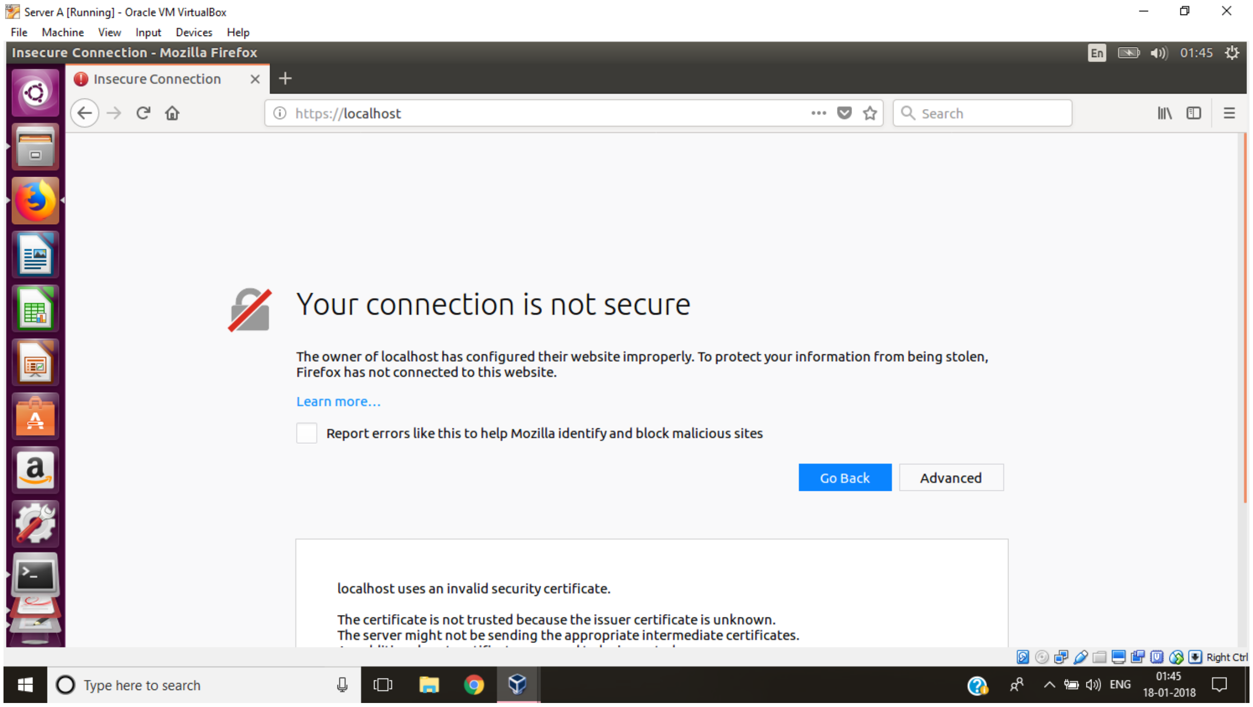
```
        Not Before: Jan 17 21:05:13 2018 GMT
        Not After : Jan 15 21:05:13 2028 GMT
    Subject: C=SE, ST=Blekinge, O=ET2540, CN=monica CA1
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
                00:b5:49:0c:1a:29:58:df:cf:c5:0c:44:1a:74:b5:
                ff:3e:01:83:c8:ae:51:5f:23:97:40:4c:d5:ee:42:
                2d:0d:76:2a:e1:d1:8f:96:fe:af:05:13:2b:eb:08:
                b1:08:0f:34:1b:7b:e8:7f:99:e8:6d:e1:2c:ec:71:
                2f:bb:70:00:26:aa:62:5b:cb:c4:f4:bd:ef:da:20:
                68:18:a8:16:31:5f:e1:10:88:0e:5e:7e:ea:6a:80:
                92:ee:d6:e5:ea:b5:fa:46:5e:9b:55:55:47:05:c9:
                65:68:a6:9e:42:de:fb:0b:e2:c2:01:db:68:b3:44:
                39:c7:d8:ef:35:6e:0a:d4:8b:a4:a9:0f:12:37:3b:
                d3:6e:e0:8e:e9:9b:4c:96:b8:fb:f2:42:49:dc:19:
                6e:2f:45:d7:3f:ae:3e:f0:4d:e3:3d:e2:94:81:36:
                e4:7a:e9:cf:a7:2c:6d:e1:13:8b:22:72:4a:d2:93:
                58:fb:09:4f:76:ec:ff:87:21:c3:f5:3c:fc:55:40:
                fe:8c:eb:a5:f8:54:28:5c:58:35:fc:4f:57:20:97:
                7e:42:86:05:1d:ad:ff:5c:1f:ab:80:71:8c:7f:ab:
                8b:0a:3f:c9:46:50:50:e8:eb:50:74:95:35:e8:61:
                a8:20:9f:e8:ac:ed:8d:c4:08:03:d5:40:68:ea:db:
                89:db:73:17:be:a7:f0:64:63:4a:22:3e:3d:39:3d:
                07:ae:86:27:b4:ea:db:43:49:da:4e:db:64:c1:5e:
                97:81:fb:2d:98:88:f8:ff:df:ba:4f:ef:b7:76:65:
                3a:a5:26:99:c4:7d:cb:2f:2b:2e:50:fc:e2:21:a6:
                12:f7:51:5b:90:d1:0c:35:f1:20:61:b9:c2:35:b1:
                48:66:e0:18:75:78:d2:04:4e:2f:e1:12:d8:e2:57:
                28:d9:00:22:74:60:3f:35:cc:1f:e9:b3:53:08:45:
                da:25:bd:21:03:a0:bb:cd:58:f7:20:f3:ec:07:6a:
                0b:07:e0:64:48:ae:52:61:6a:87:dd:07:09:b2:05:
                0e:81:f7:8e:de:0b:58:01:88:07:64:2e:34:0d:d4:
                19:88:be:df:bf:94:0a:6b:3c:a3:96:fd:d0:c9:ae:
                85:79:11:80:5e:ce:7e:d2:95:ba:01:62:06:88:07:
                13:13:d0:ff:da:73:23:e3:f4:80:db:0b:51:50:43:
```

```
            6a:41:45:8c:5d:ee:d2:ad:14:0c:1b:3d:93:4c:1f:
            4d:9c:0c:93:12:99:ce:90:f0:a8:92:bd:1e:93:00:
            0a:1f:3f:6e:66:8c:ab:3f:e4:56:5c:04:60:2a:b0:
            6f:48:7b:86:c2:03:2a:82:4d:72:3b:01:2c:80:9e:
            70:e8:8d
          Exponent: 65537 (0x10001)
      X509v3 extensions:
        X509v3 Subject Key Identifier:
          72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16
        X509v3 Authority Key Identifier:
          keyid:33:0B:E1:67:75:A9:06:A5:4E:2B:52:B1:9F:37:26:79:66:B7:7E:76

        X509v3 Basic Constraints: critical
          CA:TRUE, pathlen:0
        X509v3 Key Usage: critical
          Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
       b2:a0:11:20:33:b4:e3:05:b1:48:da:d8:8d:d2:20:14:0d:e3:
       2b:16:32:b7:4b:c0:3a:1d:d9:c5:11:94:6b:73:98:d0:8f:03:
       37:4d:31:74:42:80:10:35:ca:88:32:bd:11:7b:21:63:69:8d:
       14:d4:45:c1:7e:7c:22:24:8d:a0:3e:9b:ed:24:d5:7a:20:2c:
       3c:9f:7a:a8:a4:13:1d:8e:a0:a7:79:5b:73:1f:7c:e7:ed:4d:
       cf:cf:af:81:35:46:9c:3d:c6:64:3a:43:2c:47:6f:be:7f:b2:
       70:b4:6a:1b:a1:20:6c:25:40:d0:86:21:80:fb:9b:58:43:07:
       13:1b:b2:ba:90:86:40:8c:29:b6:7c:7f:0f:18:84:00:69:2d:
       a4:ec:88:b3:f9:e8:32:e4:f9:35:16:f2:50:fc:ed:cf:8d:62:
       46:4d:5a:d4:41:1b:41:b1:51:96:5c:3c:51:ef:6b:78:e3:90:
       dc:53:28:ca:45:88:fe:f4:33:f3:53:ba:e0:66:10:13:2e:f3:
       4f:08:6d:6f:a5:19:89:65:8c:ee:34:92:d0:41:e6:68:e7:05:
       23:da:f6:b6:53:c2:65:e1:f7:14:b1:16:d0:7e:79:c9:a8:b7:
       99:dc:e1:c5:63:bb:2c:cd:3c:fd:7c:81:d2:99:3a:a9:ac:e4:
       63:05:62:a8:dd:48:dd:62:90:62:bd:01:c7:00:26:a1:65:aa:
       67:14:71:a2:bd:96:1f:59:f0:be:ce:86:25:ab:ae:17:ca:1f:
       84:af:df:0c:e6:d2:9f:25:35:97:13:da:3d:c9:8f:fd:f9:5c:
       1f:5e:fb:bf:f8:a4:a4:dc:2b:d5:6b:c0:6c:4d:17:4c:4e:86:
       eb:ef:fd:f8:59:ef:08:39:8f:38:c7:db:4d:5c:47:c3:e9:f5:
       c6:a0:92:da:ed:d1:d3:8d:4d:26:25:4c:71:e7:4a:7d:76:4a:
```

```
0a:e0:c8:e5:36:68:f0:3a:a6:ed:2b:a1:0c:0c:92:48:cf:cf:
0e:92:20:42:9a:28:ac:e2:cc:6d:62:5c:5f:25:8f:0f:76:b4:
8c:5d:56:76:0a:8e:46:24:03:3b:c9:56:c3:f2:92:b5:58:8f:
de:ff:9e:b2:39:70:73:3f:50:5c:45:25:f4:a4:3d:c2:1f:0a:
8b:ec:d4:9d:ea:d1:2c:d0:36:22:34:ac:a9:dd:08:7a:69:d5:
08:c9:08:0b:30:a7:e3:ea:1f:8e:a4:75:ce:ff:6c:c8:d0:14:
06:2d:1c:b0:49:9a:48:3a:26:bb:70:4b:ef:37:34:0c:40:d3:
4e:0b:e5:47:27:95:c1:4d:ef:8c:a3:5f:24:71:26:30:94:ca:
3a:13:c5:da:7c:b9:52:16
```

```
ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem
ca1/certs/ca1.cert.pem
ca1/certs/ca1.cert.pem: OK
```

Task 11: Create server certificate


Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Insecure Connection - Mozilla Firefox
En
01:45
Insecure Connection
https://localhost
Search
Type here to search
ENG
01:45
18-01-2018
Right Ctrl

Your connection is not secure

The owner of localhost has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

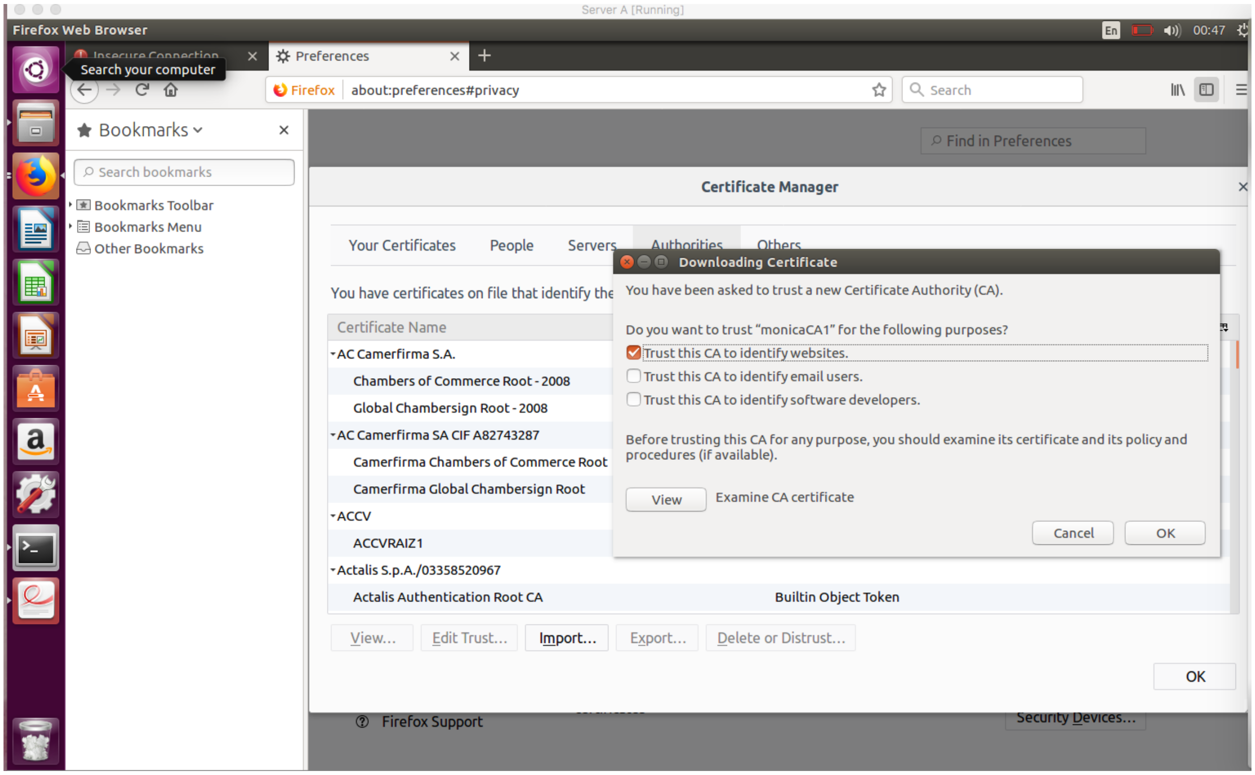
Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

Go Back   Advanced

localhost uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.



Certificate Manager

Your Certificates | People | Servers | Authorities | Others

You have certificates on file that identify the

Certificate Name	
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	
Global Chambersign Root - 2008	
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	
Camerfirma Global Chambersign Root	
ACCV	
ACCVRAIZ1	
Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token

View… | Edit Trust… | Import… | Export… | Delete or Distrust…
OK

Downloading Certificate

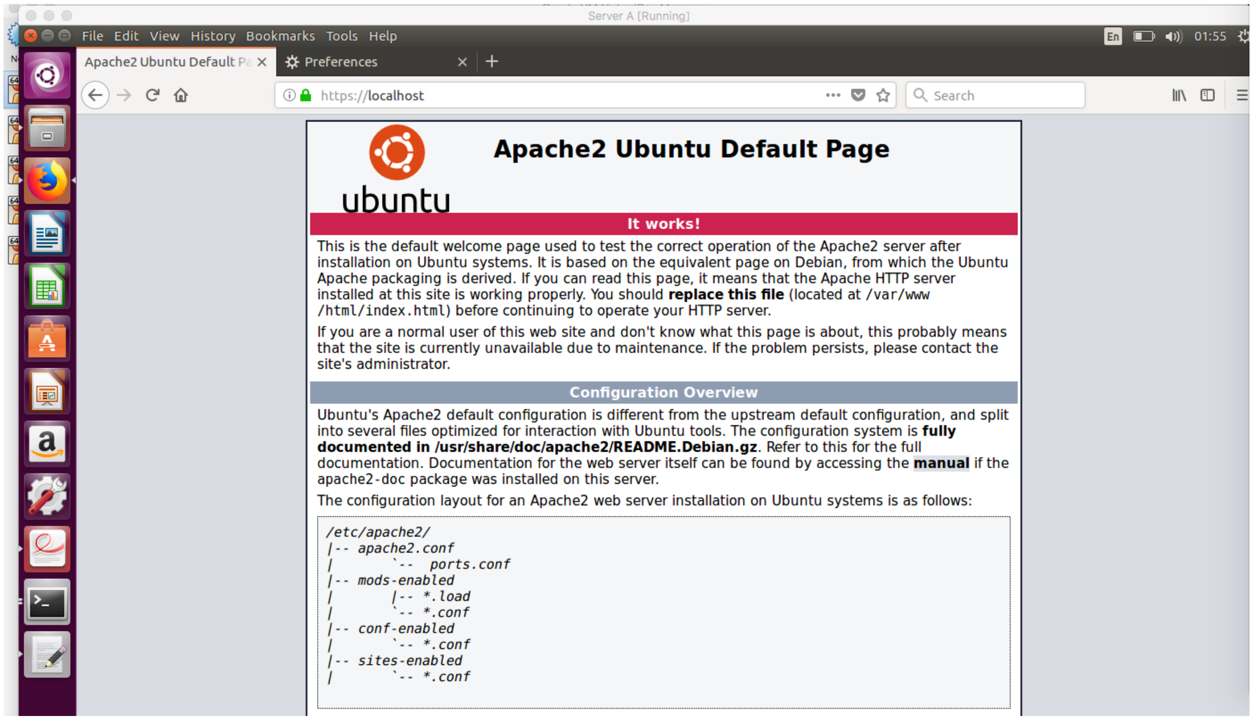
You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "monicaCA1" for the following purposes?

☑ Trust this CA to identify websites.
☐ Trust this CA to identify email users.
☐ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View | Examine CA certificate



Server A [Running]
File Edit View History Bookmarks Tools Help
01:55
Apache2 Ubuntu Default Pa
Preferences
https://localhost
Search
ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

```
ats@serverA:~/mota17_ca$ openssl genrsa -out ca1/private/ca1.server.key.pem
2048Generating RSA private key, 2048 bit long modulus
.................................+++
.............+++
e is 65537 (0x10001)


ats@serverA:~/mota17_ca$ openssl req -config ca1/openssl.cnf -new -key
ca1/private/ca1.server.key.pem  -out ca1/csr/ca1.server.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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [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 []:



ats@serverA:~/mota17_ca$ openssl req -text -noout -verify -in
ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
```

```
Data:
    Version: 0 (0x0)
    Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica CA1
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (4096 bit)
            Modulus:
                00:b5:49:0c:1a:29:58:df:cf:c5:0c:44:1a:74:b5:
                ff:3e:01:83:c8:ae:51:5f:23:97:40:4c:d5:ee:42:
                2d:0d:76:2a:e1:d1:8f:96:fe:af:05:13:2b:eb:08:
                b1:08:0f:34:1b:7b:e8:7f:99:e8:6d:e1:2c:ec:71:
                2f:bb:70:00:26:aa:62:5b:cb:c4:f4:bd:ef:da:20:
                68:18:a8:16:31:5f:e1:10:88:0e:5e:7e:ea:6a:80:
                92:ee:d6:e5:ea:b5:fa:46:5e:9b:55:55:47:05:c9:
                65:68:a6:9e:42:de:fb:0b:e2:c2:01:db:68:b3:44:
                39:c7:d8:ef:35:6e:0a:d4:8b:a4:a9:0f:12:37:3b:
                d3:6e:e0:8e:e9:9b:4c:96:b8:fb:f2:42:49:dc:19:
                6e:2f:45:d7:3f:ae:3e:f0:4d:e3:3d:e2:94:81:36:
                e4:7a:e9:cf:a7:2c:6d:e1:13:8b:22:72:4a:d2:93:
                58:fb:09:4f:76:ec:ff:87:21:c3:f5:3c:fc:55:40:
                fe:8c:eb:a5:f8:54:28:5c:58:35:fc:4f:57:20:97:
                7e:42:86:05:1d:ad:ff:5c:1f:ab:80:71:8c:7f:ab:
                8b:0a:3f:c9:46:50:50:e8:eb:50:74:95:35:e8:61:
                a8:20:9f:e8:ac:ed:8d:c4:08:03:d5:40:68:ea:db:
                89:db:73:17:be:a7:f0:64:63:4a:22:3e:3d:39:3d:
                07:ae:86:27:b4:ea:db:43:49:da:4e:db:64:c1:5e:
                97:81:fb:2d:98:88:f8:ff:df:ba:4f:ef:b7:76:65:
                3a:a5:26:99:c4:7d:cb:2f:2b:2e:50:fc:e2:21:a6:
                12:f7:51:5b:90:d1:0c:35:f1:20:61:b9:c2:35:b1:
                48:66:e0:18:75:78:d2:04:4e:2f:e1:12:d8:e2:57:
                28:d9:00:22:74:60:3f:35:cc:1f:e9:b3:53:08:45:
                da:25:bd:21:03:a0:bb:cd:58:f7:20:f3:ec:07:6a:
                0b:07:e0:64:48:ae:52:61:6a:87:dd:07:09:b2:05:
                0e:81:f7:8e:de:0b:58:01:88:07:64:2e:34:0d:d4:
                19:88:be:df:bf:94:0a:6b:3c:a3:96:fd:d0:c9:ae:
                85:79:11:80:5e:ce:7e:d2:95:ba:01:62:06:88:07:
                13:13:d0:ff:da:73:23:e3:f4:80:db:0b:51:50:43:
                6a:41:45:8c:5d:ee:d2:ad:14:0c:1b:3d:93:4c:1f:
                4d:9c:0c:93:12:99:ce:90:f0:a8:92:bd:1e:93:00:
                0a:1f:3f:6e:66:8c:ab:3f:e4:56:5c:04:60:2a:b0:
                6f:48:7b:86:c2:03:2a:82:4d:72:3b:01:2c:80:9e:
                70:e8:8d
            Exponent: 65537 (0x10001)
    Attributes:
        a0:00
Signature Algorithm: sha256WithRSAEncryption
     1d:cc:c2:70:06:a2:d2:d3:67:df:27:ca:62:6f:64:3b:3b:59:
     b5:11:58:2c:26:ab:3b:b8:aa:f4:dc:99:3e:c3:72:35:dc:33:
     e1:bf:e4:aa:2e:07:de:8b:f5:ef:ed:bd:c9:d3:3e:30:ec:5a:
     5a:82:94:27:58:a7:4e:d7:b8:12:45:c1:72:8e:a3:a9:41:c5:
     16:c8:6f:bd:e1:07:72:d4:96:35:14:86:ab:28:5a:65:a9:05:
     9c:4b:c4:91:a9:08:df:f8:b9:f6:f9:62:c6:d4:17:d9:9a:ca:
     34:5c:bf:f9:f0:22:c1:9a:6c:93:4b:de:1b:f1:ff:2b:92:61:
     3d:ba:d6:c5:1c:df:4b:f1:7e:5c:80:9c:7c:2a:55:c3:30:82:
     4f:f0:da:b0:50:b6:21:d3:7d:61:48:ed:f3:58:0f:e3:e4:72:
     47:71:a9:95:2b:d9:23:bc:bf:51:8a:42:dc:13:81:58:83:3b:
     0b:35:6a:c2:90:a8:e1:2b:f9:78:4f:63:ad:19:c7:4e:7d:9e:
     ac:fa:6d:a1:f1:fb:23:77:fd:af:9f:2b:dd:28:a1:a7:f8:fe:
     90:c2:d4:4d:38:89:a9:1d:65:63:ac:ad:8d:71:61:f4:2d:5d:
     ac:6e:da:25:93:a6:3f:1b:ec:20:56:d7:82:9c:1b:e0:fd:cd:
     f5:d5:87:f4:cb:1b:74:f4:00:ca:57:79:d5:42:76:e2:72:31:
     6c:c0:88:83:d3:0d:c7:20:1c:32:f3:4b:9d:43:b6:84:f4:99:
     8a:4e:1b:44:bc:7b:90:b8:04:9e:8c:d8:f4:43:43:d8:d0:20:
     bd:f4:a8:92:7f:ed:3c:13:13:2e:c5:81:c9:f8:39:d7:0e:44:
     91:fc:b4:40:34:c7:a7:de:d8:ef:5f:e0:df:6a:2f:db:f4:1d:
     65:0e:64:98:11:0f:db:82:52:79:ba:8d:27:90:6e:3d:e5:78:
     c8:27:19:ca:59:27:1d:8b:c7:9c:79:0e:06:e9:2d:65:6f:b5:
     6e:7a:57:c1:cd:89:45:88:08:49:bb:68:38:a4:f2:cf:f9:ff:
     e8:f8:49:4b:08:62:01:4a:55:25:50:ec:b5:aa:1b:c5:3b:52:
     e4:6a:11:43:70:76:4f:45:c7:3e:32:45:1c:45:94:3d:1d:70:
     47:52:ca:13:ff:31:d5:5f:87:47:ff:e9:48:27:c2:ad:1a:0a:
     e2:02:88:ce:30:00:d7:09:6b:90:89:d1:2b:bc:f0:f7:3e:92:
     75:39:b5:38:d1:5d:72:d6:8c:0b:48:f1:9a:c9:d1:d7:8d:8e:
     43:00:76:9b:8a:1a:4d:9e:4f:5a:ed:a9:52:ff:5d:03:9f:fb:
```

```
    7a:12:99:7f:ac:fe:08:47


ats@serverA:~/mota17_ca$ openssl ca -config ca1/openssl.cnf -extensions
server_cert -days 3650 -notext -in ca1/csr/ca1.server.csr.pem -out
ca1/certs/ca1.server.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for /home/ats/mota17_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 17 23:40:16 2018 GMT
      Not After : Jan 15 23:40:16 2028 GMT
    Subject:
      countryName               = SE
      stateOrProvinceName       = Blekinge
      localityName              = Karlskrona
      organizationName          = ET2540
      commonName                = localhost
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:
        31:EC:7C:CF:35:48:0E:F3:21:5D:5E:FC:9F:89:7B:01:DF:9D:88:A6
      X509v3 Authority Key Identifier:
        keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16
        DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=monica Root
        serial:10:00

      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication
Certificate is to be certified until Jan 15 23:40:16 2028 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
Data Base Updated


ats@serverA:~/mota17_ca$ openssl x509 -noout -text -in
ca1/certs/ca1.server.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8193 (0x2001)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, O=ET2540, CN=monica CA1
        Validity
            Not Before: Jan 17 23:40:16 2018 GMT
            Not After : Jan 15 23:40:16 2028 GMT
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:98:cb:c1:24:ee:bc:ee:f2:0d:b4:85:28:05:5d:
                    37:aa:8e:dc:43:85:d2:6e:01:da:62:5c:90:48:ff:
                    8d:38:91:4f:32:68:a3:45:9b:43:a7:e3:64:e1:63:
                    13:b7:26:1d:8d:c6:a7:9c:ed:d0:b0:74:11:62:17:
                    cd:db:d2:f7:8e:34:83:28:b4:6a:ac:50:0d:27:50:
                    d4:e2:d1:36:35:65:44:b6:e9:bd:a5:6a:67:e6:07:
                    e7:84:93:69:75:d5:81:5b:1e:81:df:3e:13:97:a2:
                    eb:dd:1c:5d:c3:e1:8e:6a:ba:a1:40:f9:2e:cc:ff:
                    9f:7d:2f:2b:79:b6:b3:fc:e6:47:2c:d5:50:f3:40:
                    65:5c:80:3f:dd:53:80:80:51:e6:ee:46:ba:af:b9:
                    68:78:88:d1:44:81:63:c5:8f:04:4b:02:ce:9c:d6:
                    78:e4:52:3d:68:ab:33:79:e4:34:91:98:e3:99:48:
                    24:51:a9:59:75:1e:d4:18:6f:ac:5c:c8:b0:9e:17:
                    d2:33:f7:14:df:a4:ff:4a:b5:fa:1f:67:d2:00:89:
```

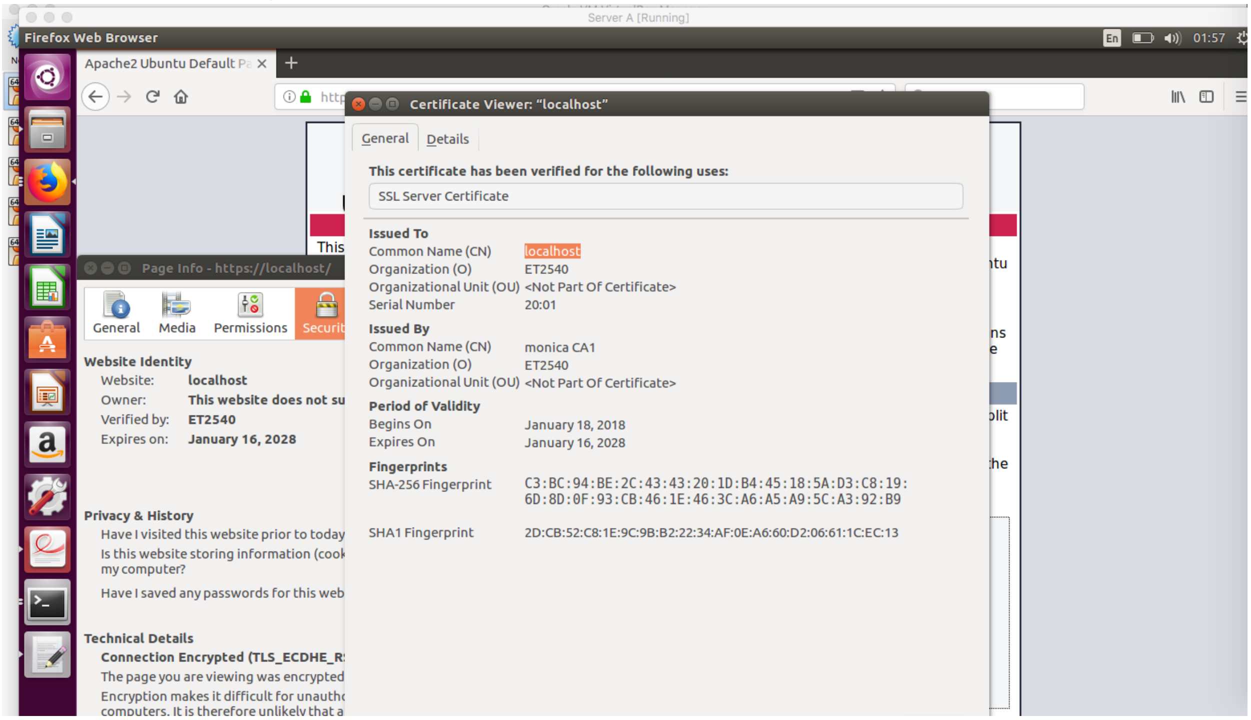
```
                    8b:90:d4:a7:8e:63:32:5d:5a:df:47:32:6e:b5:aa:
                    5e:59:e2:d4:9c:1e:35:ec:c2:aa:47:33:30:73:83:
                    e6:58:42:0e:f9:af:2f:d5:65:45:68:11:a2:99:d3:
                    4d:7d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                31:EC:7C:CF:35:48:0E:F3:21:5D:5E:FC:9F:89:7B:01:DF:9D:88:A6
            X509v3 Authority Key Identifier:
                keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16
                DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=monica Root
                serial:10:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         0e:96:4a:f5:f6:c5:8b:a0:63:5c:43:d6:20:0d:27:8b:fe:ec:
         67:4f:54:1d:c7:52:70:8a:0e:15:a1:7a:5e:5e:bf:0a:3a:6d:
         8f:48:35:c9:3b:24:d5:db:07:06:0e:b8:50:e3:07:41:db:c9:
         c5:3b:99:92:13:06:e0:33:b7:f0:87:3f:46:d5:f8:cf:20:2b:
         2f:1a:73:ae:3a:fa:7e:ce:cf:f1:a1:97:7a:c1:f3:2d:2b:46:
         cc:5b:11:07:10:a4:8f:61:c4:02:45:79:69:a3:13:5c:4d:4c:
         dc:75:30:89:24:0e:69:f9:cc:9e:f7:93:69:f6:bf:6b:88:88:
         43:41:85:9c:3e:a8:3f:fe:ac:8d:7b:d4:03:60:ed:f0:73:21:
         e1:a1:6f:89:08:5a:ae:79:c4:8e:ae:f0:bc:b0:89:f9:6c:45:
         35:dd:fd:16:b6:94:78:4b:dd:ea:af:1a:0d:16:4f:04:d6:43:
         ff:93:b4:a4:38:4d:27:5c:4f:b1:b5:5e:24:a8:a7:c4:6b:cd:
         55:b0:d1:4d:0a:89:10:57:ca:90:a8:76:33:37:b1:59:87:a6:
         2f:74:5e:d0:97:fc:a6:1a:af:4c:96:90:92:69:b0:ab:ad:4c:
         98:41:2b:31:72:09:7d:db:65:11:ea:a0:5a:09:3b:59:f2:d9:
         a7:b7:8a:2f:23:9f:30:ab:67:db:a3:62:86:64:2f:0c:48:9e:
         af:ec:d7:9f:20:7b:cf:9c:b1:70:6f:5f:43:3f:53:5e:68:5d:
         db:bd:d1:ec:18:2e:2b:69:f6:15:65:b9:3c:83:65:28:3d:3b:
```

```
77:25:9a:2c:54:aa:81:bc:03:e3:e1:d4:30:d3:14:41:75:12:
8c:ac:17:da:1a:64:d3:b5:63:4d:ce:51:0b:8a:46:da:2c:f3:
54:50:08:38:04:53:ad:0e:3c:86:ff:b0:fe:fa:69:ff:44:82:
f0:6d:6d:fc:59:08:84:68:a7:17:e4:60:78:eb:c0:9b:fc:df:
e6:64:9e:34:8c:52:4e:eb:6e:b7:73:95:23:80:00:b0:0e:cd:
11:e1:3a:f3:cb:74:8e:49:ff:f0:da:79:42:bc:8d:46:ce:40:
00:76:2b:eb:63:c7:7e:e1:de:07:c6:c0:02:fa:8c:d4:16:36:
69:b2:19:a7:76:37:86:ae:44:03:25:2e:e2:c1:0e:be:2f:2a:
89:8a:ae:c1:27:68:28:7b:42:c0:9b:a1:d4:81:e1:d1:29:83:
17:ef:b3:ae:e2:c1:c7:d5:e2:50:7a:dd:27:e7:9e:ac:16:a5:
e2:7b:30:91:de:93:ea:8a:05:f2:33:de:4b:0a:06:af:cd:ba:
e0:eb:13:02:5d:6d:10:1e
```

```
ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem -untrusted
ca1/certs/ca1.cert.pem ca1/certs/ca1.server.cert.pem
ca1/certs/ca1.server.cert.pem: OK
```

```
ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem -untrusted
ca1/certs/ca1.cert-chain.pem ca1/certs/ca1.server.cert.pem
ca1/certs/ca1.server.cert.pem: OK
```

Task 12: Show your certificate in Firefox



Website Identity
Website: localhost
Owner: This website does not su
Verified by: ET2540
Expires on: January 16, 2028

Privacy & History
Have I visited this website prior to today
Is this website storing information (cook my computer?
Have I saved any passwords for this web

Technical Details
Connection Encrypted (TLS_ECDHE_R
The page you are viewing was encrypted
Encryption makes it difficult for unauth computers. It is therefore unlikely that a

This certificate has been verified for the following uses:
SSL Server Certificate

Issued To
Common Name (CN) localhost
Organization (O) ET2540
Organizational Unit (OU) <Not Part Of Certificate>
Serial Number 20:01

Issued By
Common Name (CN) monica CA1
Organization (O) ET2540
Organizational Unit (OU) <Not Part Of Certificate>

Period of Validity
Begins On January 18, 2018
Expires On January 16, 2028

Fingerprints
SHA-256 Fingerprint C3:BC:94:BE:2C:43:43:20:1D:B4:45:18:5A:D3:C8:19:6D:8D:0F:93:CB:46:1E:46:3C:A6:A5:A9:5C:A3:92:B9
SHA1 Fingerprint 2D:CB:52:C8:1E:9C:9B:B2:22:34:AF:0E:A6:60:D2:06:61:1C:EC:13

Task 13: Create a CRL for CA1

```
ats@serverA:~/mota17_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SE/ST=Blekinge/O=ET2540/CN=monica CA1
        Last Update: Jan 18 01:01:28 2018 GMT
        Next Update: Feb 17 01:01:28 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8192
No Revoked Certificates.
    Signature Algorithm: sha256WithRSAEncryption
         a7:cb:ab:13:47:e3:ec:1b:fe:19:bf:39:2b:60:e0:5a:89:33:
         d3:90:ba:02:ed:64:07:37:8c:9d:ad:6d:03:eb:f2:3a:24:79:
         26:9d:85:81:c8:03:df:ae:eb:e9:0a:04:ed:76:90:f2:92:3c:
         fe:a0:70:49:f9:a8:a8:77:16:8d:72:8d:45:2f:54:dc:32:ed:
         13:f5:3c:ce:5e:bf:49:c6:f0:77:31:97:d1:9e:b1:36:59:4c:
         d4:75:99:09:86:de:88:14:c5:c9:ae:0a:ef:d7:1f:ec:95:61:
         ca:7a:19:30:04:af:5c:b9:9d:9a:8a:cf:40:7f:d1:3e:a0:76:
         b9:6e:6e:43:17:51:c3:45:d7:b8:2e:f6:5c:68:51:4f:5f:9b:
         0c:f0:45:1f:77:5c:bd:83:e9:03:f2:88:64:cf:f7:f7:d7:3d:
         fe:2c:d3:ad:5b:44:d9:b8:a8:b5:bf:f1:b7:61:06:af:f6:d2:
         2f:a6:d3:cb:06:bf:12:39:6f:7d:28:33:55:d6:ae:70:0b:be:
         79:87:e0:f7:ac:ae:09:a1:bd:fe:d7:d9:b7:e6:24:58:65:6e:
         e8:26:b7:48:a5:5e:40:45:09:2a:17:a3:59:b6:ae:c9:5c:7e:
         dc:b7:0c:ac:c6:07:f9:59:19:4c:8b:74:84:22:60:43:b6:9f:
         de:b7:3f:8e:50:3f:7f:22:16:06:84:6b:82:70:3b:52:11:6a:
         27:38:f8:37:86:28:54:31:de:44:fe:fa:b0:2a:62:91:53:c5:
         b7:ab:b6:00:e0:cb:ef:60:51:25:cc:44:3d:75:6e:40:1f:a8:
         00:82:7e:06:8c:2b:59:4f:fb:7f:65:42:b9:c3:0a:22:61:3f:
```

```
        ed:67:42:65:a5:86:46:39:b0:a1:15:3e:25:56:70:f5:73:6b:
        6e:1f:f2:7f:4b:10:76:12:7c:4a:56:f1:f7:11:41:0b:ef:3e:
        99:1b:de:45:e9:91:19:ba:7e:61:2f:1a:26:75:5c:c1:df:58:
        98:c4:4d:79:6c:87:02:a0:8b:da:9c:b9:99:6d:b3:24:ba:76:
        aa:0f:ea:e8:a5:d6:f3:4a:2a:03:96:93:ab:8e:d4:d7:ad:84:
        ac:c0:02:27:e2:39:0b:66:10:32:38:e8:9a:13:d4:71:e0:c9:
        ea:fe:85:29:f7:5a:ea:e0:fb:7a:8f:e9:1c:ee:33:76:6f:7d:
        05:c7:05:d6:4d:54:ac:56:fb:96:e2:22:62:09:2d:b1:e7:cc:
        a4:13:5c:f4:d3:0a:50:82:b8:e4:04:6c:3b:14:f5:8a:5a:2c:
        36:5d:94:08:87:4c:9d:2c:30:82:65:1b:83:81:71:e4:55:e7:
        1b:72:45:ee:e8:5e:e3:07
```

Task 14: Revoke a certificate

```
ats@serverA:~/mota17_ca$ openssl genrsa -out
ca1/private/ca1.server1.key.pem 2048
Generating RSA private key, 2048 bit long modulus
..........................................................................................................
......+++
............+++
e is 65537 (0x10001)


ats@serverA:~/mota17_ca$ openssl req -config ca1/openssl.cnf -new -
key ca1/private/ca1.server1.key.pem  -out ca1/csr/ca1.server1.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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:dragos.ilie@bth.se
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:


ats@serverA:~/mota17_ca$ openssl req -text -noout -verify -in
ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica
CA1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b5:49:0c:1a:29:58:df:cf:c5:0c:44:1a:74:b5:
                    ff:3e:01:83:c8:ae:51:5f:23:97:40:4c:d5:ee:42:
                    2d:0d:76:2a:e1:d1:8f:96:fe:af:05:13:2b:eb:08:
                    b1:08:0f:34:1b:7b:e8:7f:99:e8:6d:e1:2c:ec:71:
                    2f:bb:70:00:26:aa:62:5b:cb:c4:f4:bd:ef:da:20:
                    68:18:a8:16:31:5f:e1:10:88:0e:5e:7e:ea:6a:80:
                    92:ee:d6:e5:ea:b5:fa:46:5e:9b:55:55:47:05:c9:
```

```
                    65:68:a6:9e:42:de:fb:0b:e2:c2:01:db:68:b3:44:
                    39:c7:d8:ef:35:6e:0a:d4:8b:a4:a9:0f:12:37:3b:
                    d3:6e:e0:8e:e9:9b:4c:96:b8:fb:f2:42:49:dc:19:
                    6e:2f:45:d7:3f:ae:3e:f0:4d:e3:3d:e2:94:81:36:
                    e4:7a:e9:cf:a7:2c:6d:e1:13:8b:22:72:4a:d2:93:
                    58:fb:09:4f:76:ec:ff:87:21:c3:f5:3c:fc:55:40:
                    fe:8c:eb:a5:f8:54:28:5c:58:35:fc:4f:57:20:97:
                    7e:42:86:05:1d:ad:ff:5c:1f:ab:80:71:8c:7f:ab:
                    8b:0a:3f:c9:46:50:50:e8:eb:50:74:95:35:e8:61:
                    a8:20:9f:e8:ac:ed:8d:c4:08:03:d5:40:68:ea:db:
                    89:db:73:17:be:a7:f0:64:63:4a:22:3e:3d:39:3d:
                    07:ae:86:27:b4:ea:db:43:49:da:4e:db:64:c1:5e:
                    97:81:fb:2d:98:88:f8:ff:df:ba:4f:ef:b7:76:65:
                    3a:a5:26:99:c4:7d:cb:2f:2b:2e:50:fc:e2:21:a6:
                    12:f7:51:5b:90:d1:0c:35:f1:20:61:b9:c2:35:b1:
                    48:66:e0:18:75:78:d2:04:4e:2f:e1:12:d8:e2:57:
                    28:d9:00:22:74:60:3f:35:cc:1f:e9:b3:53:08:45:
                    da:25:bd:21:03:a0:bb:cd:58:f7:20:f3:ec:07:6a:
                    0b:07:e0:64:48:ae:52:61:6a:87:dd:07:09:b2:05:
                    0e:81:f7:8e:de:0b:58:01:88:07:64:2e:34:0d:d4:
                    19:88:be:df:bf:94:0a:6b:3c:a3:96:fd:d0:c9:ae:
                    85:79:11:80:5e:ce:7e:d2:95:ba:01:62:06:88:07:
                    13:13:d0:ff:da:73:23:e3:f4:80:db:0b:51:50:43:
                    6a:41:45:8c:5d:ee:d2:ad:14:0c:1b:3d:93:4c:1f:
                    4d:9c:0c:93:12:99:ce:90:f0:a8:92:bd:1e:93:00:
                    0a:1f:3f:6e:66:8c:ab:3f:e4:56:5c:04:60:2a:b0:
                    6f:48:7b:86:c2:03:2a:82:4d:72:3b:01:2c:80:9e:
                    70:e8:8d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         1d:cc:c2:70:06:a2:d2:d3:67:df:27:ca:62:6f:64:3b:3b:59:
```

```
         b5:11:58:2c:26:ab:3b:b8:aa:f4:dc:99:3e:c3:72:35:dc:33:
         e1:bf:e4:aa:2e:07:de:8b:f5:ef:ed:bd:c9:d3:3e:30:ec:5a:
         5a:82:94:27:58:a7:4e:d7:b8:12:45:c1:72:8e:a3:a9:41:c5:
         16:c8:6f:bd:e1:07:72:d4:96:35:14:86:ab:28:5a:65:a9:05:
         9c:4b:c4:91:a9:08:df:f8:b9:f6:f9:62:c6:d4:17:d9:9a:ca:
         34:5c:bf:f9:f0:22:c1:9a:6c:93:4b:de:1b:f1:ff:2b:92:61:
         3d:ba:d6:c5:1c:df:4b:f1:7e:5c:80:9c:7c:2a:55:c3:30:82:
         4f:f0:da:b0:50:b6:21:d3:7d:61:48:ed:f3:58:0f:e3:e4:72:
         47:71:a9:95:2b:d9:23:bc:bf:51:8a:42:dc:13:81:58:83:3b:
         0b:35:6a:c2:90:a8:e1:2b:f9:78:4f:63:ad:19:c7:4e:7d:9e:
         ac:fa:6d:a1:f1:fb:23:77:fd:af:9f:2b:dd:28:a1:a7:f8:fe:
         90:c2:d4:4d:38:89:a9:1d:65:63:ac:ad:8d:71:61:f4:2d:5d:
         ac:6e:da:25:93:a6:3f:1b:ec:20:56:d7:82:9c:1b:e0:fd:cd:
         f5:d5:87:f4:cb:1b:74:f4:00:ca:57:79:d5:42:76:e2:72:31:
         6c:c0:88:83:d3:0d:c7:20:1c:32:f3:4b:9d:43:b6:84:f4:99:
         8a:4e:1b:44:bc:7b:90:b8:04:9e:8c:d8:f4:43:43:d8:d0:20:
         bd:f4:a8:92:7f:ed:3c:13:13:2e:c5:81:c9:f8:39:d7:0e:44:
         91:fc:b4:40:34:c7:a7:de:d8:ef:5f:e0:df:6a:2f:db:f4:1d:
         65:0e:64:98:11:0f:db:82:52:79:ba:8d:27:90:6e:3d:e5:78:
         c8:27:19:ca:59:27:1d:8b:c7:9c:79:0e:06:e9:2d:65:6f:b5:
         6e:7a:57:c1:cd:89:45:88:08:49:bb:68:38:a4:f2:cf:f9:ff:
         e8:f8:49:4b:08:62:01:4a:55:25:50:ec:b5:aa:1b:c5:3b:52:
         e4:6a:11:43:70:76:4f:45:c7:3e:32:45:1c:45:94:3d:1d:70:
         47:52:ca:13:ff:31:d5:5f:87:47:ff:e9:48:27:c2:ad:1a:0a:
         e2:02:88:ce:30:00:d7:09:6b:90:89:d1:2b:bc:f0:f7:3e:92:
         75:39:b5:38:d1:5d:72:d6:8c:0b:48:f1:9a:c9:d1:d7:8d:8e:
         43:00:76:9b:8a:1a:4d:9e:4f:5a:ed:a9:52:ff:5d:03:9f:fb:
         7a:12:99:7f:ac:fe:08:47


ats@serverA:~/mota17_ca$ openssl ca -config ca1/openssl.cnf -
extensions usr_cert -days 3650 -notext -in ca1/csr/ca1.server1.csr.pem
-out ca1/certs/ca1.server1.cert.pem
```

```
Using configuration from ca1/openssl.cnf
Enter pass phrase for
/home/ats/mota17_ca/ca1//private/ca1.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8194 (0x2002)
        Validity
            Not Before: Jan 18 01:12:44 2018 GMT
            Not After : Jan 16 01:12:44 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            localityName              = Karlskrona
            organizationName          = ET2540
            commonName                = dragos.ilie@bth.se
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:

0E:89:1F:0C:2B:9C:CC:97:D3:BD:7B:F4:DE:0E:8B:F8:C3:9E:B7:9D
            X509v3 Authority Key Identifier:

keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16

            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
Certificate is to be certified until Jan 16 01:12:44 2028 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
Data Base Updated


ats@serverA:~/mota17_ca$ openssl x509 -noout -text -in
ca1/certs/ca1.server1.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8194 (0x2002)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, O=ET2540, CN=monica CA1
        Validity
            Not Before: Jan 18 01:12:44 2018 GMT
            Not After : Jan 16 01:12:44 2028 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:
                    00:ce:21:ee:0c:80:09:6d:df:6d:f7:18:07:09:17:
                    d9:92:f5:4a:b9:75:68:d8:ae:a8:d9:5e:6a:5f:0c:
                    b9:2e:f5:e5:93:2c:32:42:a1:f4:2c:b1:bb:ca:ec:
                    87:21:6f:d0:ce:bc:b0:51:1b:c4:83:9b:62:10:bc:
                    b1:1a:22:a6:2a:d6:9f:2f:67:b8:a2:ce:8c:9f:47:
                    b2:bb:b2:91:fc:23:32:0c:1d:83:23:41:fe:30:94:
                    a6:51:c3:93:ef:59:15:3a:0e:02:5d:eb:7a:e6:92:
                    88:cd:b5:f7:a8:51:83:49:57:93:41:40:ba:86:b6:
```

```
                    4e:3b:2d:b9:da:76:6e:c8:df:76:bd:41:2f:30:69:
                    cf:1e:a5:7e:af:9f:0f:d3:38:41:23:b0:1e:04:cf:
                    dd:2c:e7:52:5e:71:6f:0a:df:76:d5:b4:9f:8a:ad:
                    06:c3:79:a4:75:a5:e1:c8:ba:c8:a0:fe:4e:82:8c:
                    99:01:a4:d6:1b:ce:cb:32:3e:88:9e:d7:87:df:63:
                    77:23:fa:f0:db:a1:7c:eb:2f:0c:78:93:dd:da:aa:
                    70:5d:bd:46:8f:24:68:b1:23:26:d7:ef:3a:a0:89:
                    66:e1:12:bd:d9:8c:c8:ab:71:39:90:e9:c1:12:59:
                    58:9e:c9:2b:d8:ad:7e:54:d6:39:bc:1f:25:d3:e3:
                    00:cf
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:

0E:89:1F:0C:2B:9C:CC:97:D3:BD:7B:F4:DE:0E:8B:F8:C3:9E:B7:9D
            X509v3 Authority Key Identifier:

keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16

            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
    Signature Algorithm: sha256WithRSAEncryption
         00:5c:36:2f:07:57:a0:da:53:7f:63:18:68:96:36:9e:b3:30:
         04:07:58:8f:fc:1d:5e:0f:aa:1f:c1:2f:05:62:c5:dd:98:2e:
         a9:95:0c:8e:26:4b:eb:6a:ed:ad:a9:35:0c:e1:65:67:e7:17:
         41:4b:49:89:a8:c5:ac:71:49:35:3a:31:e9:1c:3f:df:1c:16:
         f6:de:d8:94:7a:df:91:f6:08:7f:38:85:90:54:eb:a2:89:63:
```

```
         bf:57:c0:2d:78:6e:fa:67:1e:0b:8f:72:4f:67:06:61:61:3c:
         ce:d5:8e:fe:bb:44:4f:1a:0b:21:a0:3d:e2:cb:5c:67:71:6c:
         b5:c9:1b:1e:2f:ab:09:92:4a:db:39:30:c8:06:54:48:f2:fb:
         c8:38:b9:b1:60:33:a3:e2:8d:3c:bc:83:26:16:26:b4:bf:9f:
         17:96:fe:cd:b1:0f:6d:b7:af:d9:4c:32:ea:44:0f:21:be:43:
         f4:40:88:41:1a:d7:09:7e:da:b4:c6:e4:58:e1:c2:a5:a4:19:
         6a:92:64:e2:31:53:8c:b4:75:32:bd:56:22:37:88:83:df:ff:
         59:8a:b7:fe:06:fd:d4:d0:f8:94:fe:48:fb:7b:cc:4f:cf:5f:
         b3:73:59:7b:96:d3:0e:4a:42:2e:ed:a4:f6:50:c4:d8:a2:2b:
         30:4d:7d:a4:73:35:df:26:cf:7d:7d:c7:99:5a:65:c7:82:8e:
         ae:a2:93:ee:24:d5:78:b0:0a:b4:c7:08:dc:f0:35:8a:70:52:
         1d:dd:c6:7d:8d:c6:6d:9e:e4:60:14:fe:a2:a9:ab:ae:02:6b:
         85:7c:07:cf:ab:83:0f:4a:ff:3c:97:28:5d:b6:25:fb:e9:28:
         39:0d:49:18:2b:94:e6:8b:48:7c:ad:c4:76:f7:36:df:a8:78:
         1d:9e:5c:9f:44:2f:d4:5d:a8:b5:bf:0c:23:d7:21:7a:c5:38:
         7e:a5:81:42:f3:c4:a3:e7:b4:83:00:37:ba:94:18:62:a6:2f:
         f1:fb:c2:aa:11:51:55:9d:c7:20:53:90:99:88:09:58:e1:1f:
         21:34:74:e7:bb:94:46:41:2b:c4:9d:0f:51:d1:0d:06:4d:15:
         77:1a:b4:16:59:80:a4:6d:2c:86:f8:68:39:44:3d:06:dc:4a:
         4c:d8:63:84:b0:6a:cf:be:de:a4:88:b9:6b:fb:0c:56:0c:8c:
         dc:06:33:bc:3c:4f:17:d1:19:81:54:31:5d:2b:66:fb:74:83:
         56:49:44:00:a2:51:7e:0b:d2:1b:75:26:14:44:76:d0:97:e4:
         56:ab:05:e1:c0:71:8a:ea:7e:73:7d:72:e6:7e:fb:63:de:3d:
         34:b7:47:67:c0:8c:31:76
```

```
ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem -
untrusted ca1/certs/ca1.cert.pem ca1/certs/ca1.server1.cert.pem
ca1/certs/ca1.server1.cert.pem: OK
```

```
ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem -
untrusted ca1/certs/ca1.cert-chain.pem
ca1/certs/ca1.server1.cert.pem
ca1/certs/ca1.server1.cert.pem: OK
```

```
ats@serverA:~/mota17_ca$ openssl ca -config ca1/openssl.cnf -revoke
ca1/certs/ca1.server1.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for
/home/ats/mota17_ca/ca1//private/ca1.key.pem:
Revoking Certificate 2002.
Data Base Updated
```

```
ats@serverA:~/mota17_ca$ openssl ca -config ca1/openssl.cnf -gencrl -
out ca1/crl/ca1.crl.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for
/home/ats/mota17_ca/ca1//private/ca1.key.pem:
```

```
ats@serverA:~/mota17_ca/ca1$ cat report
V       280115232304Z           2000 unknown
        /C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=moni
V       280115234016Z           2001 unknown
        /C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=localhost
R       280116011244Z 180118011825Z 2002 unknown
        /C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=dragos.ilie@bth.s
e
```

```
ats@serverA:~/mota17_ca$ openssl crl -in ca1/crl/ca1.crl.pem -noout -
text
```

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: /C=SE/ST=Blekinge/O=ET2540/CN=monica CA1
        Last Update: Jan 18 01:28:41 2018 GMT
        Next Update: Feb 17 01:28:41 2018 GMT
        CRL extensions:
            X509v3 CRL Number:
                8193
Revoked Certificates:
    Serial Number: 2002
        Revocation Date: Jan 18 01:18:25 2018 GMT
    Signature Algorithm: sha256WithRSAEncryption
         3e:96:61:8a:83:6d:30:6d:11:96:f2:81:cf:d2:0e:1d:76:53:
         c9:1d:56:20:ce:11:47:3c:d8:f8:94:81:c4:ae:b4:e9:78:4a:
         55:ec:5f:5c:24:85:ae:f6:84:2f:1e:29:9b:ee:5b:87:f1:fa:
         d1:b4:aa:7a:de:4b:76:51:79:66:2a:1c:50:80:a9:d5:48:4c:
         17:15:94:1f:80:58:05:3a:64:28:1b:2d:17:0f:7c:1c:ae:8a:
         25:8a:a8:57:71:77:ed:de:71:46:bf:08:69:74:7a:41:14:a5:
         0c:d9:38:2e:0c:75:64:3d:6a:d9:06:93:ab:a4:13:03:1b:b0:
         c8:dd:bc:78:05:20:58:02:6a:7c:ba:86:a7:b0:62:c9:bc:d8:
         27:44:d9:24:e6:d3:1f:fd:06:33:25:39:95:dc:a4:b7:dc:a0:
         af:79:20:4b:7b:d1:a4:89:a7:76:70:1f:3f:71:f0:21:b5:d8:
         ac:46:ae:7a:d2:71:4a:b4:41:f5:47:56:a8:0b:1b:2c:88:a9:
         de:0e:19:13:3a:6a:e8:79:07:de:3c:0b:0f:f2:b5:2e:db:53:
         57:b2:1a:02:4d:d4:2c:a5:4f:b1:5b:48:e9:c5:c7:38:1e:e1:
         bb:0b:f4:c3:b6:12:83:31:67:1e:2f:7b:d6:05:47:09:9c:b7:
         80:d4:47:80:49:6d:a9:5a:e8:4f:b1:e1:7f:c7:77:76:23:62:
         9d:f8:30:f5:92:7f:cf:4a:a5:b6:7f:b5:36:ea:ca:f6:47:2c:
         52:00:b8:cf:e2:2e:3b:c7:ed:be:61:ac:a2:cb:fe:8d:2a:82:
         13:ac:91:82:f6:26:f5:80:95:4b:a0:28:b1:ff:8f:2e:32:07:
         95:ae:c4:1f:28:2e:55:4e:b1:f7:47:cf:e1:e8:86:31:c1:21:
         d4:14:f2:05:58:3f:5c:86:52:15:69:69:c4:88:e4:39:be:1a:
```

```
        4c:74:1f:ef:38:1a:1e:8e:85:04:30:7b:89:0b:e9:97:4c:b8:
        9a:03:62:8f:c2:cb:67:59:51:ba:f7:2f:e5:ec:07:23:a6:92:
        a1:d5:c1:ee:a1:a1:bc:de:5d:55:67:d7:70:f9:13:ce:a7:e9:
        64:28:1a:12:95:3a:23:1f:18:8e:f0:66:d5:e3:bc:c4:3f:c2:
        5b:6e:d5:5d:4f:a4:2b:0c:e9:e9:75:d6:15:9e:67:cf:ea:e4:
        81:78:2c:88:d4:d8:6d:4e:86:7e:ed:bf:f9:9f:41:c6:ed:b6:
        10:94:1f:3b:4d:9d:bd:e7:9e:ef:ae:80:80:df:c4:e8:15:d7:
        70:ca:03:75:93:76:16:e1:7d:61:9b:4d:10:41:8b:cf:3c:59:
        53:8a:80:05:3a:5a:ae:e0
```

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

```
ats@serverA:/etc$ sudo cat 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 "atslabb00"
```

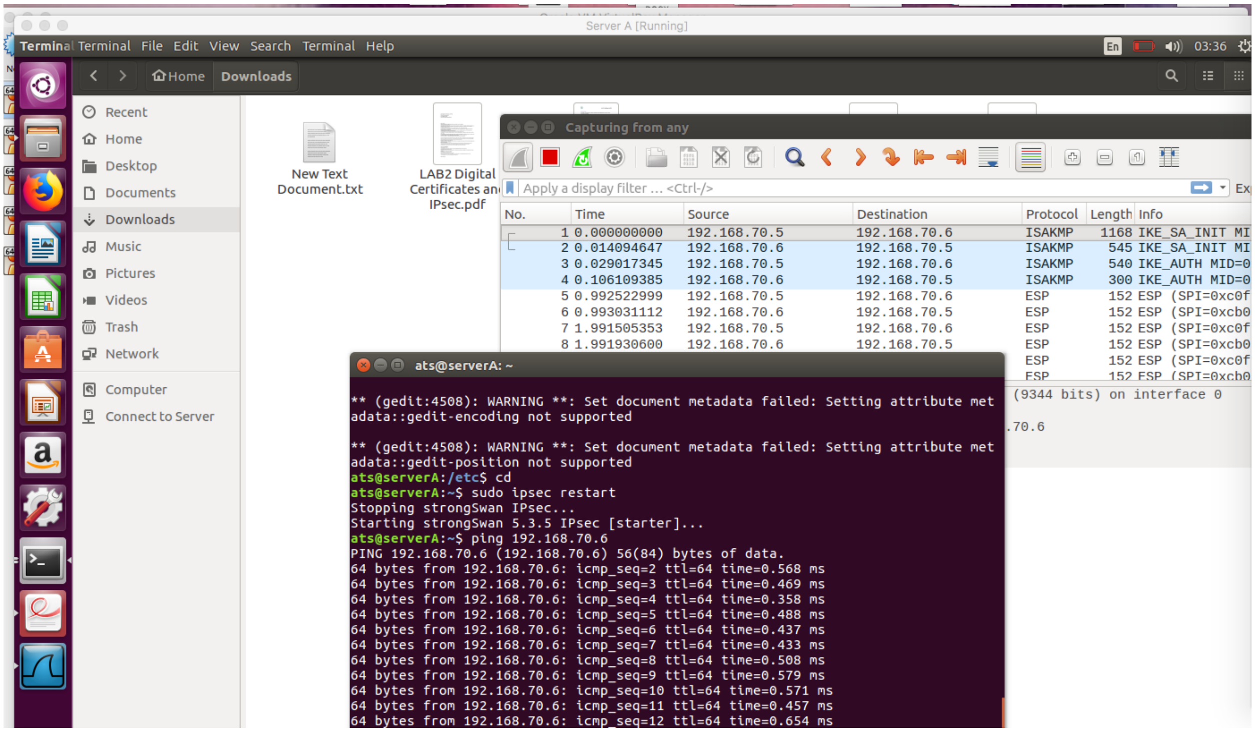
```
ats@serverA:/etc$ sudo cat ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# 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=selfCert.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=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 serverA-serverB
        auto=route
        authby=psk
        type=transport
        keyexchange=ikev2
        left=192.168.70.5
        right=192.168.70.6
```

ServerB

```
ats@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 "atslabb00"
```

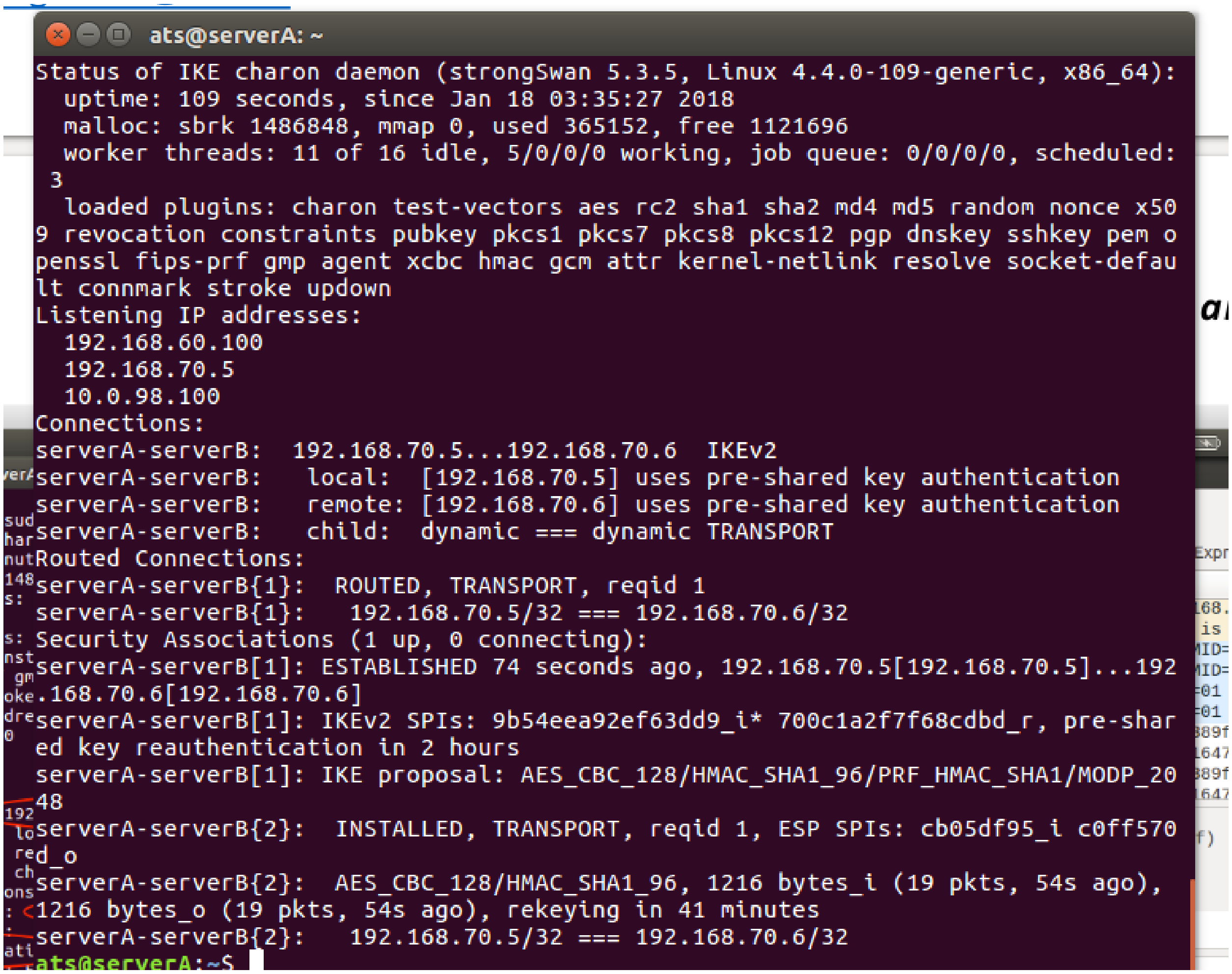
```
ats@serverB:~$ sudo cat /etc/ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup
conn serverB- to-serverA
auto=route
authby=psk
type=transport
keyexchange=ikev2
left=192.168.70.6
right=192.168.70.5
```



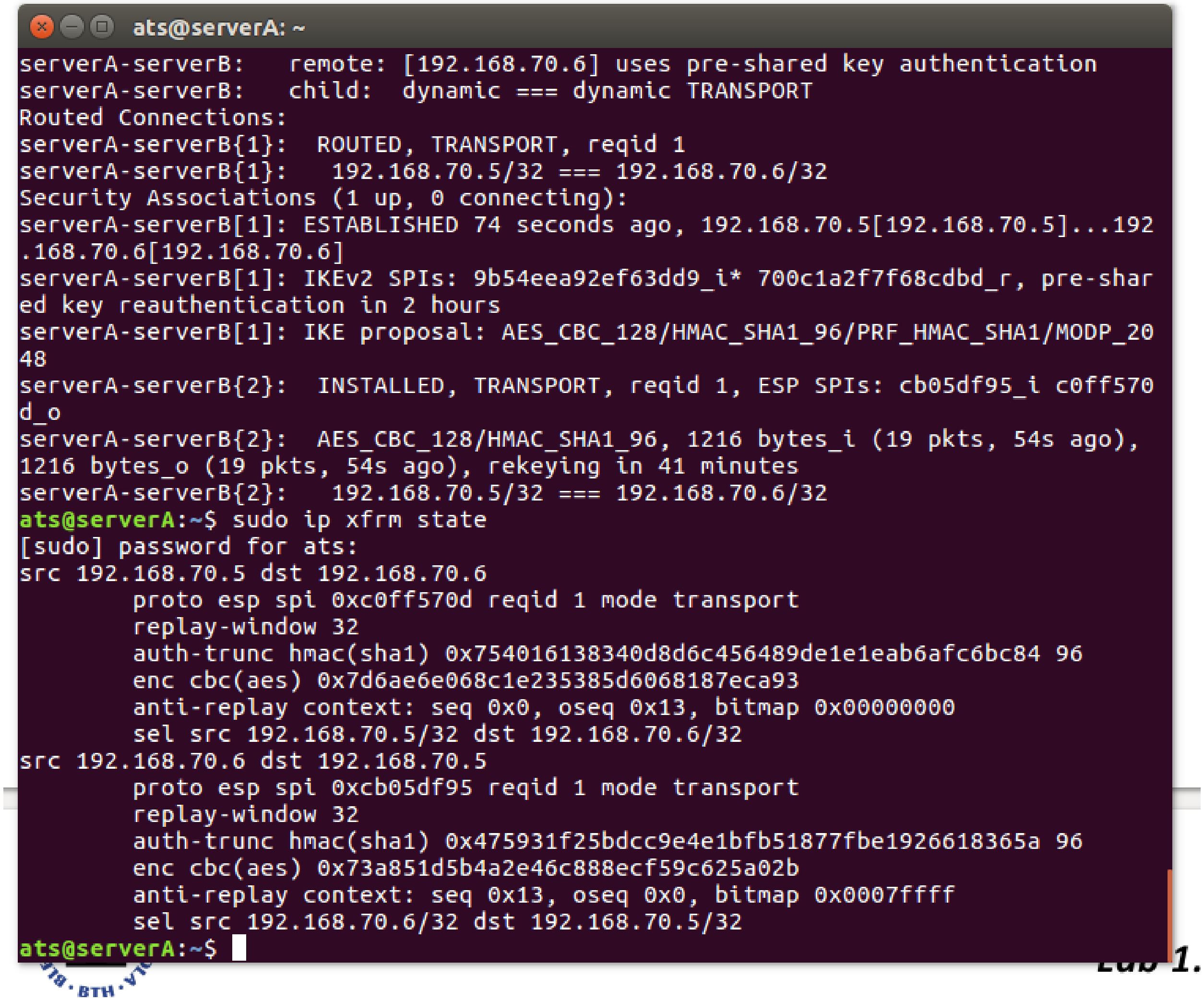
```
No.   Time          Source          Destination     Protocol  Length Info
    1 0.000000000   192.168.70.5    192.168.70.6    ISAKMP     1168 IKE_SA_INIT MI
    2 0.014094647   192.168.70.6    192.168.70.5    ISAKMP      545 IKE_SA_INIT MI
    3 0.029017345   192.168.70.5    192.168.70.6    ISAKMP      540 IKE_AUTH MID=0
    4 0.106109385   192.168.70.6    192.168.70.5    ISAKMP      300 IKE_AUTH MID=0
    5 0.992522999   192.168.70.5    192.168.70.6    ESP         152 ESP (SPI=0xc0f
    6 0.993031112   192.168.70.6    192.168.70.5    ESP         152 ESP (SPI=0xcb0
    7 1.991505353   192.168.70.5    192.168.70.6    ESP         152 ESP (SPI=0xc0f
    8 1.991930600   192.168.70.6    192.168.70.5    ESP         152 ESP (SPI=0xcb0
                                                    ESP         152 ESP (SPI=0xc0f
                                                    ESP         152 ESP (SPI=0xcb0
(9344 bits) on interface 0
.70.6
```

```
ats@serverA: ~

** (gedit:4508): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-encoding not supported

** (gedit:4508): WARNING **: Set document metadata failed: Setting attribute met
adata::gedit-position not supported
ats@serverA:/etc$ cd
ats@serverA:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.3.5 IPsec [starter]...
ats@serverA:~$ ping 192.168.70.6
PING 192.168.70.6 (192.168.70.6) 56(84) bytes of data.
64 bytes from 192.168.70.6: icmp_seq=2 ttl=64 time=0.568 ms
64 bytes from 192.168.70.6: icmp_seq=3 ttl=64 time=0.469 ms
64 bytes from 192.168.70.6: icmp_seq=4 ttl=64 time=0.358 ms
64 bytes from 192.168.70.6: icmp_seq=5 ttl=64 time=0.488 ms
64 bytes from 192.168.70.6: icmp_seq=6 ttl=64 time=0.437 ms
64 bytes from 192.168.70.6: icmp_seq=7 ttl=64 time=0.433 ms
64 bytes from 192.168.70.6: icmp_seq=8 ttl=64 time=0.508 ms
64 bytes from 192.168.70.6: icmp_seq=9 ttl=64 time=0.579 ms
64 bytes from 192.168.70.6: icmp_seq=10 ttl=64 time=0.571 ms
64 bytes from 192.168.70.6: icmp_seq=11 ttl=64 time=0.457 ms
64 bytes from 192.168.70.6: icmp_seq=12 ttl=64 time=0.654 ms
```

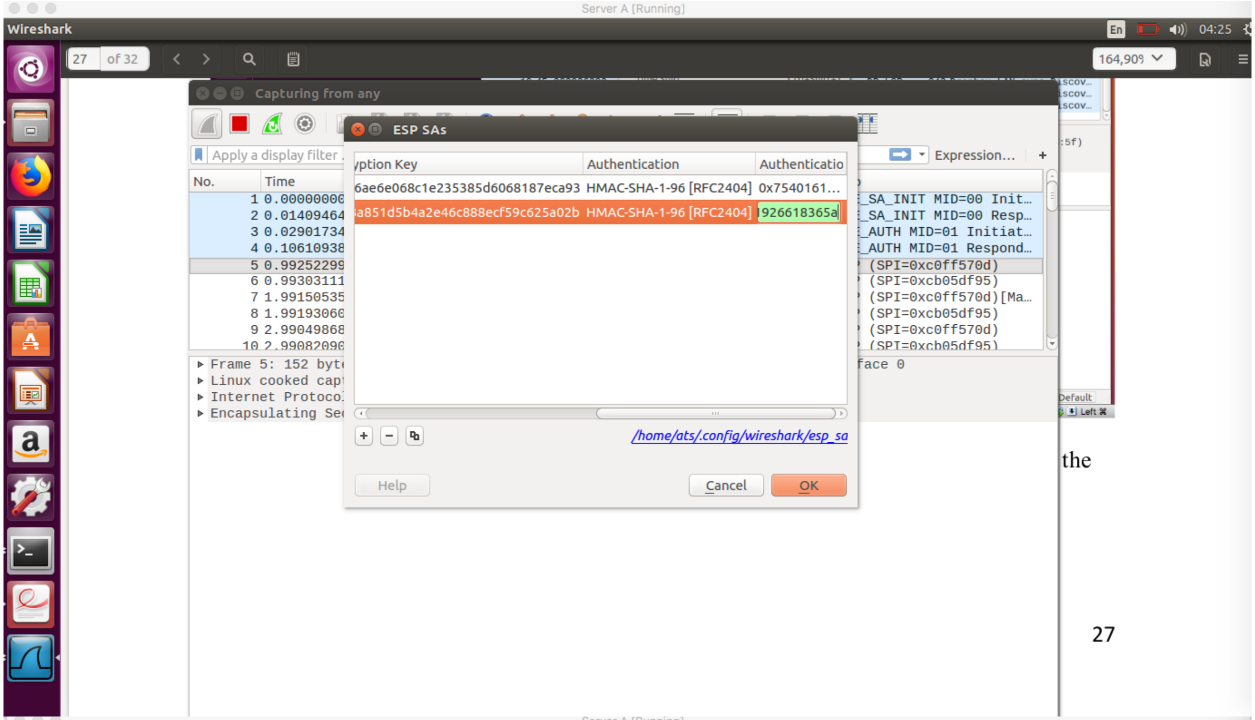
Task 16: Decrypt traffic with Wireshark



```
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-109-generic, x86_64):
  uptime: 109 seconds, since Jan 18 03:35:27 2018
  malloc: sbrk 1486848, mmap 0, used 365152, free 1121696
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled:
 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x50
9 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem o
penssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-defau
lt connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-serverB:  192.168.70.5...192.168.70.6  IKEv2
serverA-serverB:   local:  [192.168.70.5] uses pre-shared key authentication
serverA-serverB:   remote: [192.168.70.6] uses pre-shared key authentication
serverA-serverB:   child:  dynamic === dynamic TRANSPORT
Routed Connections:
serverA-serverB{1}:  ROUTED, TRANSPORT, reqid 1
serverA-serverB{1}:   192.168.70.5/32 === 192.168.70.6/32
Security Associations (1 up, 0 connecting):
serverA-serverB[1]: ESTABLISHED 74 seconds ago, 192.168.70.5[192.168.70.5]...192
.168.70.6[192.168.70.6]
serverA-serverB[1]: IKEv2 SPIs: 9b54eea92ef63dd9_i* 700c1a2f7f68cdbd_r, pre-shar
ed key reauthentication in 2 hours
serverA-serverB[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_20
48
serverA-serverB{2}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: cb05df95_i c0ff570
d_o
serverA-serverB{2}:  AES_CBC_128/HMAC_SHA1_96, 1216 bytes_i (19 pkts, 54s ago),
1216 bytes_o (19 pkts, 54s ago), rekeying in 41 minutes
serverA-serverB{2}:   192.168.70.5/32 === 192.168.70.6/32
ats@serverA:~$
```



```
serverA-serverB:   remote: [192.168.70.6] uses pre-shared key authentication
serverA-serverB:   child:  dynamic === dynamic TRANSPORT
Routed Connections:
serverA-serverB{1}:  ROUTED, TRANSPORT, reqid 1
serverA-serverB{1}:   192.168.70.5/32 === 192.168.70.6/32
Security Associations (1 up, 0 connecting):
serverA-serverB[1]: ESTABLISHED 74 seconds ago, 192.168.70.5[192.168.70.5]...192
.168.70.6[192.168.70.6]
serverA-serverB[1]: IKEv2 SPIs: 9b54eea92ef63dd9_i* 700c1a2f7f68cdbd_r, pre-shar
ed key reauthentication in 2 hours
serverA-serverB[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_20
48
serverA-serverB{2}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: cb05df95_i c0ff570
d_o
serverA-serverB{2}:  AES_CBC_128/HMAC_SHA1_96, 1216 bytes_i (19 pkts, 54s ago),
1216 bytes_o (19 pkts, 54s ago), rekeying in 41 minutes
serverA-serverB{2}:   192.168.70.5/32 === 192.168.70.6/32
ats@serverA:~$ sudo ip xfrm state
[sudo] password for ats:
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc0ff570d reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x754016138340d8d6c456489de1e1eab6afc6bc84 96
        enc cbc(aes) 0x7d6ae6e068c1e235385d6068187eca93
        anti-replay context: seq 0x0, oseq 0x13, 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 spi 0xcb05df95 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x475931f25bdcc9e4e1bfb51877fbe1926618365a 96
        enc cbc(aes) 0x73a851d5b4a2e46c888ecf59c625a02b
        anti-replay context: seq 0x13, oseq 0x0, bitmap 0x0007ffff
        sel src 192.168.70.6/32 dst 192.168.70.5/32
ats@serverA:~$ 
```

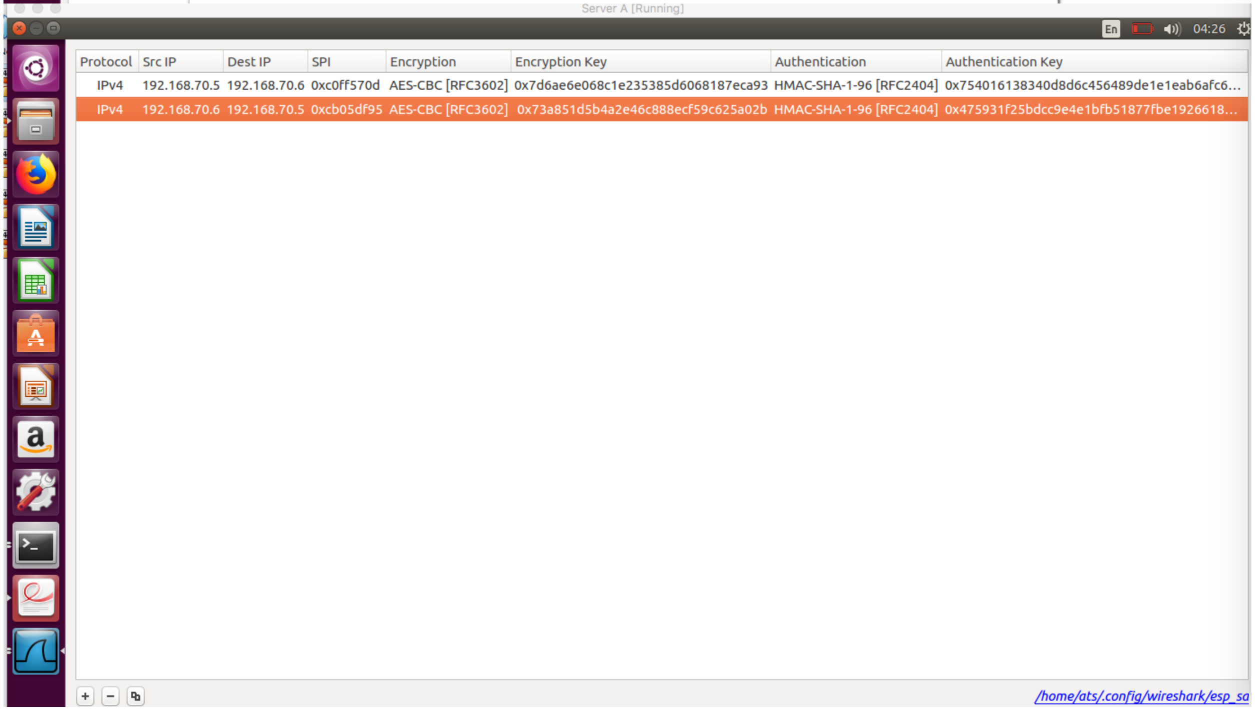


ESP SAs

…ption Key	Authentication	Authenticatio…
6ae6e068c1e235385d6068187eca93	HMAC-SHA-1-96 [RFC2404]	0x7540161…
…a851d5b4a2e46c888ecf59c625a02b	HMAC-SHA-1-96 [RFC2404]	…926618365a

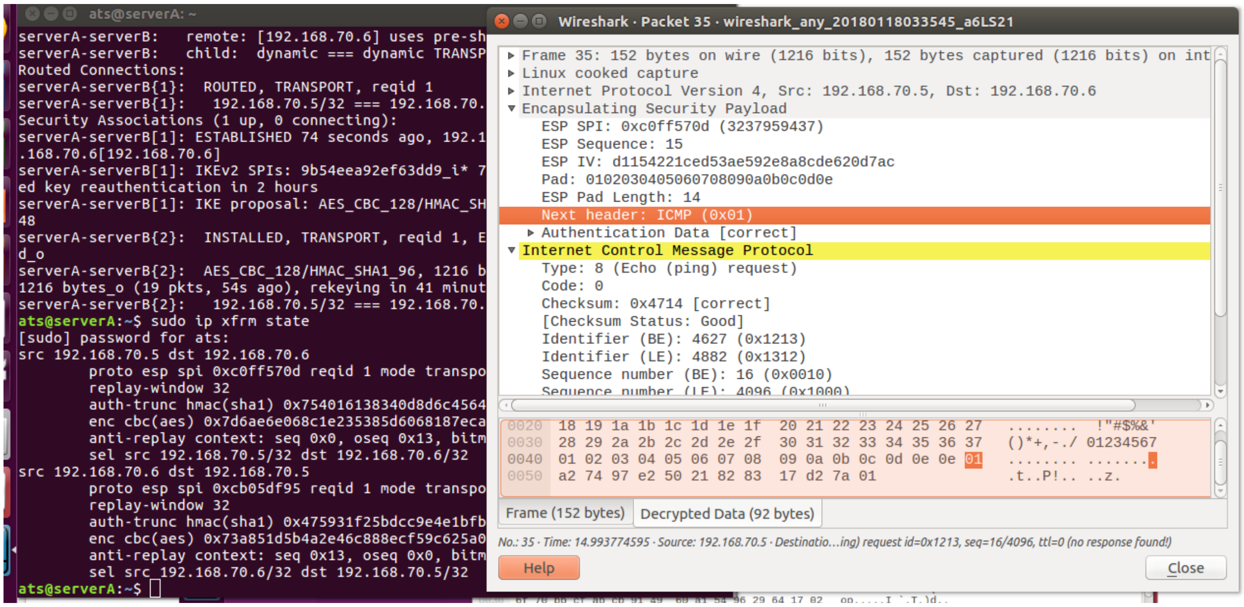
/home/ats/.config/wireshark/esp_sa

```
No.  Time
 1 0.00000000…   …_SA_INIT MID=00 Init…
 2 0.01409464    …_SA_INIT MID=00 Resp…
 3 0.02901734    …_AUTH MID=01 Initiat…
 4 0.10610938    …_AUTH MID=01 Respond…
 5 0.99252299    … (SPI=0xc0ff570d)
 6 0.99303111    … (SPI=0xcb05df95)
 7 1.99150535    … (SPI=0xc0ff570d)[Ma…
 8 1.99193060    … (SPI=0xcb05df95)
 9 2.99049868    … (SPI=0xc0ff570d)
10 2.99082090    … (SPI=0xcb05df95)
▸ Frame 5: 152 byt…                …face 0
▸ Linux cooked cap…
▸ Internet Protoco…
▸ Encapsulating Se…
```



Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key	Authentication	Authentication Key
IPv4	192.168.70.5	192.168.70.6	0xc0ff570d	AES-CBC [RFC3602]	0x7d6ae6e068c1e235385d6068187eca93	HMAC-SHA-1-96 [RFC2404]	0x754016138340d8d6c456489de1e1eab6afc6…
IPv4	192.168.70.6	192.168.70.5	0xcb05df95	AES-CBC [RFC3602]	0x73a851d5b4a2e46c888ecf59c625a02b	HMAC-SHA-1-96 [RFC2404]	0x475931f25bdcc9e4e1bfb51877fbe1926618…

/home/ats/.config/wireshark/esp_sa


ats@serverA: ~
Wireshark · Packet 35 · wireshark_any_20180118033545_a6LS21
Frame (152 bytes)
Decrypted Data (92 bytes)
Help
Close

```
serverA-serverB:   remote: [192.168.70.6] uses pre-sh
serverA-serverB:   child:  dynamic === dynamic TRANSP
Routed Connections:
serverA-serverB{1}:  ROUTED, TRANSPORT, reqid 1
serverA-serverB{1}:   192.168.70.5/32 === 192.168.70.
Security Associations (1 up, 0 connecting):
serverA-serverB[1]: ESTABLISHED 74 seconds ago, 192.1
.168.70.6[192.168.70.6]
serverA-serverB[1]: IKEv2 SPIs: 9b54eea92ef63dd9_i* 7
ed key reauthentication in 2 hours
serverA-serverB[1]: IKE proposal: AES_CBC_128/HMAC_SH
48
serverA-serverB{2}:  INSTALLED, TRANSPORT, reqid 1, E
d_o
serverA-serverB{2}:  AES_CBC_128/HMAC_SHA1_96, 1216 b
1216 bytes_o (19 pkts, 54s ago), rekeying in 41 minut
serverA-serverB{2}:   192.168.70.5/32 === 192.168.70.
ats@serverA:~$ sudo ip xfrm state
[sudo] password for ats:
src 192.168.70.5 dst 192.168.70.6
        proto esp spi 0xc0ff570d reqid 1 mode transpo
        replay-window 32
        auth-trunc hmac(sha1) 0x754016138340d8d6c4564
        enc cbc(aes) 0x7d6ae6e068c1e235385d6068187eca
        anti-replay context: seq 0x0, oseq 0x13, bitm
        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 spi 0xcb05df95 reqid 1 mode transpo
        replay-window 32
        auth-trunc hmac(sha1) 0x475931f25bdcc9e4e1bfb
        enc cbc(aes) 0x73a851d5b4a2e46c888ecf59c625a0
        anti-replay context: seq 0x13, oseq 0x0, bitm
        sel src 192.168.70.6/32 dst 192.168.70.5/32
ats@serverA:~$
```

```
▶ Frame 35: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on int
▶ Linux cooked capture
▶ Internet Protocol Version 4, Src: 192.168.70.5, Dst: 192.168.70.6
▼ Encapsulating Security Payload
    ESP SPI: 0xc0ff570d (3237959437)
    ESP Sequence: 15
    ESP IV: d1154221ced53ae592e8a8cde620d7ac
    Pad: 0102030405060708090a0b0c0d0e
    ESP Pad Length: 14
    Next header: ICMP (0x01)
  ▶ Authentication Data [correct]
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4714 [correct]
    [Checksum Status: Good]
    Identifier (BE): 4627 (0x1213)
    Identifier (LE): 4882 (0x1312)
    Sequence number (BE): 16 (0x0010)
    Sequence number (LE): 4096 (0x1000)
```

```
0020  18 19 1a 1b 1c 1d 1e 1f  20 21 22 23 24 25 26 27   ........  !"#$%&'
0030  28 29 2a 2b 2c 2d 2e 2f  30 31 32 33 34 35 36 37   ()*+,-./ 01234567
0040  01 02 03 04 05 06 07 08  09 0a 0b 0c 0d 0e 0e 01   ........ ........
0050  a2 74 97 e2 50 21 82 83  17 d2 7a 01               .t..P!.. ..z.
```

No.: 35 · Time: 14.993774595 · Source: 192.168.70.5 · Destinatio…ing) request id=0x1213, seq=16/4096, ttl=0 (no response found!)

Task 17: List the entries in the SPD

Mode Transport

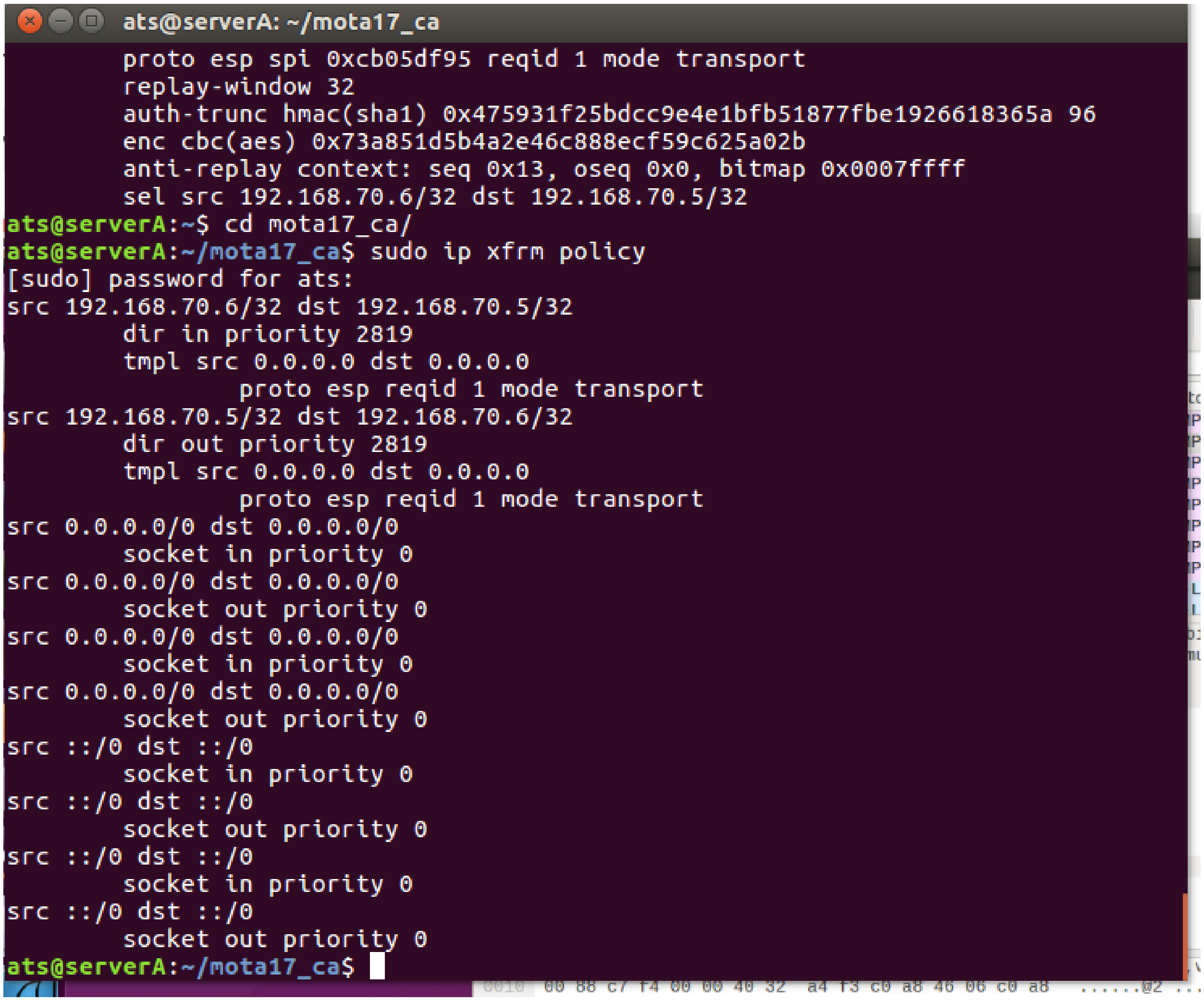
transport, signifying host-to-host transport mode.

proto esp

specifies a transform protocol: IPsec Encapsulating Security Payload (esp).

dir in

indicates direction



```
        proto esp spi 0xcb05df95 reqid 1 mode transport
        replay-window 32
        auth-trunc hmac(sha1) 0x475931f25bdcc9e4e1bfb51877fbe1926618365a 96
        enc cbc(aes) 0x73a851d5b4a2e46c888ecf59c625a02b
        anti-replay context: seq 0x13, oseq 0x0, bitmap 0x0007ffff
        sel src 192.168.70.6/32 dst 192.168.70.5/32
ats@serverA:~$ cd mota17_ca/
ats@serverA:~/mota17_ca$ sudo ip xfrm policy
[sudo] password for ats:
src 192.168.70.6/32 dst 192.168.70.5/32
        dir in priority 2819
        tmpl src 0.0.0.0 dst 0.0.0.0
                proto esp reqid 1 mode transport
src 192.168.70.5/32 dst 192.168.70.6/32
        dir out priority 2819
        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
ats@serverA:~/mota17_ca$ 
```

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

```
ats@serverA:~$ sudo cat /etc/ipsec.secrets
[sudo] password for ats:
# 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.

: RSA /etc/ipsec.d/private/ca1.serverA.key.pem"
ats@serverA:~$
```

```
sudo cat ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        charondebug="all"
        strictcrlpolicy=no
        uniqueids=yes




# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.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=myCert.pem
#      right=192.168.0.2
#      rightsubnet=10.2.0.0/16
#      rightid="C=CH, O=Linux strongSwan CN=peer name"
#      auto=start
```

```
ats@serverA:~$
```

```
ats@serverA:~/mota17_ca$ openssl genrsa -out
ca1/private/ca1.serverA.key.pem 2048
Generating RSA private key, 2048 bit long modulus
.........+++
..........+++
e is 65537 (0x10001)
```

```
ats@serverA:~/mota17_ca$ openssl req -config ca1/openssl.cnf -new -
key ca1/private/ca1.serverA.key.pem  -out ca1/csr/ca1.serverA.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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [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 []:
An optional company name []:


ats@serverA:~/mota17_ca$ openssl req -text -noout -verify -in
ca1/csr/ca1.csr.pem
verify OK
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica
CA1
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
        Modulus:
          00:b5:49:0c:1a:29:58:df:cf:c5:0c:44:1a:74:b5:
          ff:3e:01:83:c8:ae:51:5f:23:97:40:4c:d5:ee:42:
          2d:0d:76:2a:e1:d1:8f:96:fe:af:05:13:2b:eb:08:
          b1:08:0f:34:1b:7b:e8:7f:99:e8:6d:e1:2c:ec:71:
          2f:bb:70:00:26:aa:62:5b:cb:c4:f4:bd:ef:da:20:
          68:18:a8:16:31:5f:e1:10:88:0e:5e:7e:ea:6a:80:
          92:ee:d6:e5:ea:b5:fa:46:5e:9b:55:55:47:05:c9:
          65:68:a6:9e:42:de:fb:0b:e2:c2:01:db:68:b3:44:
          39:c7:d8:ef:35:6e:0a:d4:8b:a4:a9:0f:12:37:3b:
          d3:6e:e0:8e:e9:9b:4c:96:b8:fb:f2:42:49:dc:19:
          6e:2f:45:d7:3f:ae:3e:f0:4d:e3:3d:e2:94:81:36:
          e4:7a:e9:cf:a7:2c:6d:e1:13:8b:22:72:4a:d2:93:
          58:fb:09:4f:76:ec:ff:87:21:c3:f5:3c:fc:55:40:
          fe:8c:eb:a5:f8:54:28:5c:58:35:fc:4f:57:20:97:
          7e:42:86:05:1d:ad:ff:5c:1f:ab:80:71:8c:7f:ab:
```

```
                    8b:0a:3f:c9:46:50:50:e8:eb:50:74:95:35:e8:61:
                    a8:20:9f:e8:ac:ed:8d:c4:08:03:d5:40:68:ea:db:
                    89:db:73:17:be:a7:f0:64:63:4a:22:3e:3d:39:3d:
                    07:ae:86:27:b4:ea:db:43:49:da:4e:db:64:c1:5e:
                    97:81:fb:2d:98:88:f8:ff:df:ba:4f:ef:b7:76:65:
                    3a:a5:26:99:c4:7d:cb:2f:2b:2e:50:fc:e2:21:a6:
                    12:f7:51:5b:90:d1:0c:35:f1:20:61:b9:c2:35:b1:
                    48:66:e0:18:75:78:d2:04:4e:2f:e1:12:d8:e2:57:
                    28:d9:00:22:74:60:3f:35:cc:1f:e9:b3:53:08:45:
                    da:25:bd:21:03:a0:bb:cd:58:f7:20:f3:ec:07:6a:
                    0b:07:e0:64:48:ae:52:61:6a:87:dd:07:09:b2:05:
                    0e:81:f7:8e:de:0b:58:01:88:07:64:2e:34:0d:d4:
                    19:88:be:df:bf:94:0a:6b:3c:a3:96:fd:d0:c9:ae:
                    85:79:11:80:5e:ce:7e:d2:95:ba:01:62:06:88:07:
                    13:13:d0:ff:da:73:23:e3:f4:80:db:0b:51:50:43:
                    6a:41:45:8c:5d:ee:d2:ad:14:0c:1b:3d:93:4c:1f:
                    4d:9c:0c:93:12:99:ce:90:f0:a8:92:bd:1e:93:00:
                    0a:1f:3f:6e:66:8c:ab:3f:e4:56:5c:04:60:2a:b0:
                    6f:48:7b:86:c2:03:2a:82:4d:72:3b:01:2c:80:9e:
                    70:e8:8d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         1d:cc:c2:70:06:a2:d2:d3:67:df:27:ca:62:6f:64:3b:3b:59:
         b5:11:58:2c:26:ab:3b:b8:aa:f4:dc:99:3e:c3:72:35:dc:33:
         e1:bf:e4:aa:2e:07:de:8b:f5:ef:ed:bd:c9:d3:3e:30:ec:5a:
         5a:82:94:27:58:a7:4e:d7:b8:12:45:c1:72:8e:a3:a9:41:c5:
         16:c8:6f:bd:e1:07:72:d4:96:35:14:86:ab:28:5a:65:a9:05:
         9c:4b:c4:91:a9:08:df:f8:b9:f6:f9:62:c6:d4:17:d9:9a:ca:
         34:5c:bf:f9:f0:22:c1:9a:6c:93:4b:de:1b:f1:ff:2b:92:61:
         3d:ba:d6:c5:1c:df:4b:f1:7e:5c:80:9c:7c:2a:55:c3:30:82:
         4f:f0:da:b0:50:b6:21:d3:7d:61:48:ed:f3:58:0f:e3:e4:72:
```

```
         47:71:a9:95:2b:d9:23:bc:bf:51:8a:42:dc:13:81:58:83:3b:
         0b:35:6a:c2:90:a8:e1:2b:f9:78:4f:63:ad:19:c7:4e:7d:9e:
         ac:fa:6d:a1:f1:fb:23:77:fd:af:9f:2b:dd:28:a1:a7:f8:fe:
         90:c2:d4:4d:38:89:a9:1d:65:63:ac:ad:8d:71:61:f4:2d:5d:
         ac:6e:da:25:93:a6:3f:1b:ec:20:56:d7:82:9c:1b:e0:fd:cd:
         f5:d5:87:f4:cb:1b:74:f4:00:ca:57:79:d5:42:76:e2:72:31:
         6c:c0:88:83:d3:0d:c7:20:1c:32:f3:4b:9d:43:b6:84:f4:99:
         8a:4e:1b:44:bc:7b:90:b8:04:9e:8c:d8:f4:43:43:d8:d0:20:
         bd:f4:a8:92:7f:ed:3c:13:13:2e:c5:81:c9:f8:39:d7:0e:44:
         91:fc:b4:40:34:c7:a7:de:d8:ef:5f:e0:df:6a:2f:db:f4:1d:
         65:0e:64:98:11:0f:db:82:52:79:ba:8d:27:90:6e:3d:e5:78:
         c8:27:19:ca:59:27:1d:8b:c7:9c:79:0e:06:e9:2d:65:6f:b5:
         6e:7a:57:c1:cd:89:45:88:08:49:bb:68:38:a4:f2:cf:f9:ff:
         e8:f8:49:4b:08:62:01:4a:55:25:50:ec:b5:aa:1b:c5:3b:52:
         e4:6a:11:43:70:76:4f:45:c7:3e:32:45:1c:45:94:3d:1d:70:
         47:52:ca:13:ff:31:d5:5f:87:47:ff:e9:48:27:c2:ad:1a:0a:
         e2:02:88:ce:30:00:d7:09:6b:90:89:d1:2b:bc:f0:f7:3e:92:
         75:39:b5:38:d1:5d:72:d6:8c:0b:48:f1:9a:c9:d1:d7:8d:8e:
         43:00:76:9b:8a:1a:4d:9e:4f:5a:ed:a9:52:ff:5d:03:9f:fb:
         7a:12:99:7f:ac:fe:08:47


ats@serverA:~/mota17_ca$ openssl ca -config ca1/openssl.cnf -
extensions server_cert -days 3650 -notext -in
ca1/csr/ca1.serverA.csr.pem -out ca1/certs/ca1.serverA.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for
/home/ats/mota17_ca/ca1//private/ca1.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8195 (0x2003)
        Validity
```

```
            Not Before: Jan 18 04:26:10 2018 GMT
            Not After : Jan 16 04:26:10 2028 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:

4B:55:D6:41:24:F5:54:38:8D:E0:69:74:E8:2D:3A:70:85:D5:64:4F
            X509v3 Authority Key Identifier:

keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16

DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=monica Root
                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:
                  URI:https://localhost/ca1.crl.pem

Certificate is to be certified until Jan 16 04:26:10 2028 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
Data Base Updated

ats@serverA:~/mota17_ca$ openssl x509 -noout -text -in
ca1/certs/ca1.serverA.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8195 (0x2003)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, O=ET2540, CN=monica CA1
        Validity
            Not Before: Jan 18 04:26:10 2018 GMT
            Not After : Jan 16 04:26:10 2028 GMT
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d8:85:98:c8:47:42:b1:7f:0d:8e:09:01:97:07:
                    0e:94:c0:7f:e2:59:44:a6:67:41:2b:5a:16:0b:05:
                    77:be:2f:9f:85:f1:65:3e:80:f2:41:6a:ff:8b:54:
                    df:c5:bb:e8:86:14:f6:fd:91:28:e8:71:79:43:5a:
                    a3:22:0a:42:dc:d4:cd:43:8f:a2:22:20:f7:2c:4e:
                    ab:65:f4:a2:de:35:0e:bf:00:89:fd:7c:56:9c:81:
                    9e:4d:4b:88:39:12:82:40:d6:40:5d:82:94:37:80:
                    3b:59:38:a8:c2:01:2c:97:38:46:81:13:bc:7d:a5:
                    e4:2a:9f:59:93:6f:18:ee:6e:91:9e:f3:ed:67:47:
                    1d:c1:d4:c0:bf:96:85:25:79:08:f3:5b:28:10:97:
                    8b:f0:87:25:48:40:2f:2e:76:5c:4c:8e:50:00:31:
```

```
          26:bd:4f:cb:8e:0c:17:86:00:49:fa:a6:ee:d6:fe:
          bc:bc:db:19:10:5c:ea:ca:b0:21:bb:37:af:2b:63:
          97:3b:7b:d6:70:e2:59:78:e9:74:e2:c4:11:20:60:
          82:8f:4d:5b:1f:d4:fd:65:a8:54:da:72:38:4d:cd:
          1e:d2:ec:80:38:38:b9:38:d5:c9:4f:84:5c:45:f8:
          4e:0a:55:7c:66:65:64:dd:c1:52:84:82:03:5c:e3:
          4a:db
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:

4B:55:D6:41:24:F5:54:38:8D:E0:69:74:E8:2D:3A:70:85:D5:64:4F
      X509v3 Authority Key Identifier:

keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16

DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=monica Root
        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:
         URI:https://localhost/ca1.crl.pem

  Signature Algorithm: sha256WithRSAEncryption
     17:c8:c0:33:94:2a:44:68:d7:aa:af:42:eb:e4:69:0b:59:ca:
     e3:16:84:fd:81:9a:8b:31:ee:c4:4f:c0:c2:1c:e2:19:46:63:
     e8:13:3e:8a:d0:9c:02:ed:8c:a8:78:1d:77:19:42:1b:52:e0:
     2b:76:0f:bb:a4:97:c4:f5:ab:14:93:c3:ba:94:ed:f6:2b:46:
     44:5e:87:0a:69:68:82:b5:79:c7:44:f5:36:42:70:b5:51:e5:
     e9:d4:c2:ab:ee:60:4a:3b:59:f0:21:57:e8:32:3c:bb:4b:13:
     6b:25:65:5f:0f:05:2c:4b:6f:6b:b4:04:f6:c3:56:20:57:d2:
     93:e3:ea:da:8d:43:2c:f8:13:88:10:1b:75:ba:02:61:39:3d:
     a3:05:dc:50:c6:09:f3:fc:07:46:04:aa:f7:c9:bb:9c:53:51:
     0c:66:54:62:7a:75:c7:39:b9:bf:c1:7e:93:2a:d9:93:ae:a0:
     26:a4:68:ae:e2:ab:80:c8:69:6b:c9:32:16:14:0f:06:d7:21:
     eb:cf:2b:2f:2e:36:e6:ed:4a:3a:01:21:38:99:60:20:06:3c:
     df:15:c2:b2:b4:35:78:bc:48:90:88:78:86:b8:f8:00:70:4c:
     0d:55:8a:95:ac:6e:fa:43:11:20:41:de:76:a4:2c:45:43:a8:
     b1:b0:62:cd:92:78:ae:49:fe:7e:86:24:42:87:4f:bf:82:29:
     f5:5b:2c:f4:2c:31:9b:b0:63:08:0f:b1:d5:c5:f4:b9:cf:ee:
     c8:af:24:5c:47:61:5e:c1:62:b6:80:c0:70:4e:90:fb:fd:92:
     06:07:b6:6a:55:40:43:62:e9:40:ff:b7:03:65:a0:61:d7:0c:
     83:eb:cf:70:7c:8a:e9:67:40:23:0f:ed:5b:30:c1:66:d0:f6:
     71:94:57:f4:7b:8a:d4:a0:0a:e8:6a:b0:02:1e:9f:d6:6b:00:
     b8:9c:fd:17:55:ef:8a:92:9e:46:03:b3:fb:ca:1c:a7:3c:f8:
     44:b6:04:b7:d4:ce:28:6b:70:f0:f4:78:86:2f:11:af:b4:26:
     02:41:11:b5:9e:3e:08:0d:86:57:fc:86:85:1d:69:a4:1c:8c:
     96:d7:f7:8e:a7:e5:e8:05:16:22:1b:bd:2a:ae:43:4e:df:0a:
     2a:f4:c8:e5:4f:cc:30:31:29:d2:4a:25:fe:6c:72:2a:72:8a:
     a8:8c:91:ef:24:c6:64:2f:ce:a8:f1:c5:3e:92:33:70:d4:6e:
     ef:06:98:23:41:00:ed:f3:61:7f:98:c2:0a:1c:8a:45:a7:ac:
     96:1e:aa:f1:66:bd:0d:65:de:1d:b9:77:87:f2:bc:c9:a2:eb:
     5d:5b:c5:0a:56:39:9f:d6

ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem -
untrusted ca1/certs/ca1.cert.pem ca1/certs/ca1.serverA.cert.pem
ca1/certs/ca1.serverA.cert.pem: OK
```

```
ats@serverA:~/mota17_ca$ openssl genrsa -out
ca1/private/ca1.serverB.key.pem 2048
Generating RSA private key, 2048 bit long modulus
..........+++
...............................................................................+++
e is 65537 (0x10001)

ats@serverA:~/mota17_ca$ openssl req -config ca1/openssl.cnf -new -
key ca1/private/ca1.serverB.key.pem  -out ca1/csr/ca1.serverB.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) [SE]:
State or Province Name (full name) [Blekinge]:
Locality Name (eg, city) [Karlskrona]:
Organization Name (eg, company) [ET2540]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:192.168.70.6
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

ats@serverA:~/mota17_ca$ openssl req -text -noout -verify -in
ca1/csr/ca1.csr.pem
```

```
verify OK
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica
CA1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b5:49:0c:1a:29:58:df:cf:c5:0c:44:1a:74:b5:
                    ff:3e:01:83:c8:ae:51:5f:23:97:40:4c:d5:ee:42:
                    2d:0d:76:2a:e1:d1:8f:96:fe:af:05:13:2b:eb:08:
                    b1:08:0f:34:1b:7b:e8:7f:99:e8:6d:e1:2c:ec:71:
                    2f:bb:70:00:26:aa:62:5b:cb:c4:f4:bd:ef:da:20:
                    68:18:a8:16:31:5f:e1:10:88:0e:5e:7e:ea:6a:80:
                    92:ee:d6:e5:ea:b5:fa:46:5e:9b:55:55:47:05:c9:
                    65:68:a6:9e:42:de:fb:0b:e2:c2:01:db:68:b3:44:
                    39:c7:d8:ef:35:6e:0a:d4:8b:a4:a9:0f:12:37:3b:
                    d3:6e:e0:8e:e9:9b:4c:96:b8:fb:f2:42:49:dc:19:
                    6e:2f:45:d7:3f:ae:3e:f0:4d:e3:3d:e2:94:81:36:
                    e4:7a:e9:cf:a7:2c:6d:e1:13:8b:22:72:4a:d2:93:
                    58:fb:09:4f:76:ec:ff:87:21:c3:f5:3c:fc:55:40:
                    fe:8c:eb:a5:f8:54:28:5c:58:35:fc:4f:57:20:97:
                    7e:42:86:05:1d:ad:ff:5c:1f:ab:80:71:8c:7f:ab:
                    8b:0a:3f:c9:46:50:50:e8:eb:50:74:95:35:e8:61:
                    a8:20:9f:e8:ac:ed:8d:c4:08:03:d5:40:68:ea:db:
                    89:db:73:17:be:a7:f0:64:63:4a:22:3e:3d:39:3d:
                    07:ae:86:27:b4:ea:db:43:49:da:4e:db:64:c1:5e:
                    97:81:fb:2d:98:88:f8:ff:df:ba:4f:ef:b7:76:65:
                    3a:a5:26:99:c4:7d:cb:2f:2b:2e:50:fc:e2:21:a6:
                    12:f7:51:5b:90:d1:0c:35:f1:20:61:b9:c2:35:b1:
                    48:66:e0:18:75:78:d2:04:4e:2f:e1:12:d8:e2:57:
```

```
                    28:d9:00:22:74:60:3f:35:cc:1f:e9:b3:53:08:45:
                    da:25:bd:21:03:a0:bb:cd:58:f7:20:f3:ec:07:6a:
                    0b:07:e0:64:48:ae:52:61:6a:87:dd:07:09:b2:05:
                    0e:81:f7:8e:de:0b:58:01:88:07:64:2e:34:0d:d4:
                    19:88:be:df:bf:94:0a:6b:3c:a3:96:fd:d0:c9:ae:
                    85:79:11:80:5e:ce:7e:d2:95:ba:01:62:06:88:07:
                    13:13:d0:ff:da:73:23:e3:f4:80:db:0b:51:50:43:
                    6a:41:45:8c:5d:ee:d2:ad:14:0c:1b:3d:93:4c:1f:
                    4d:9c:0c:93:12:99:ce:90:f0:a8:92:bd:1e:93:00:
                    0a:1f:3f:6e:66:8c:ab:3f:e4:56:5c:04:60:2a:b0:
                    6f:48:7b:86:c2:03:2a:82:4d:72:3b:01:2c:80:9e:
                    70:e8:8d
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
         1d:cc:c2:70:06:a2:d2:d3:67:df:27:ca:62:6f:64:3b:3b:59:
         b5:11:58:2c:26:ab:3b:b8:aa:f4:dc:99:3e:c3:72:35:dc:33:
         e1:bf:e4:aa:2e:07:de:8b:f5:ef:ed:bd:c9:d3:3e:30:ec:5a:
         5a:82:94:27:58:a7:4e:d7:b8:12:45:c1:72:8e:a3:a9:41:c5:
         16:c8:6f:bd:e1:07:72:d4:96:35:14:86:ab:28:5a:65:a9:05:
         9c:4b:c4:91:a9:08:df:f8:b9:f6:f9:62:c6:d4:17:d9:9a:ca:
         34:5c:bf:f9:f0:22:c1:9a:6c:93:4b:de:1b:f1:ff:2b:92:61:
         3d:ba:d6:c5:1c:df:4b:f1:7e:5c:80:9c:7c:2a:55:c3:30:82:
         4f:f0:da:b0:50:b6:21:d3:7d:61:48:ed:f3:58:0f:e3:e4:72:
         47:71:a9:95:2b:d9:23:bc:bf:51:8a:42:dc:13:81:58:83:3b:
         0b:35:6a:c2:90:a8:e1:2b:f9:78:4f:63:ad:19:c7:4e:7d:9e:
         ac:fa:6d:a1:f1:fb:23:77:fd:af:9f:2b:dd:28:a1:a7:f8:fe:
         90:c2:d4:4d:38:89:a9:1d:65:63:ac:ad:8d:71:61:f4:2d:5d:
         ac:6e:da:25:93:a6:3f:1b:ec:20:56:d7:82:9c:1b:e0:fd:cd:
         f5:d5:87:f4:cb:1b:74:f4:00:ca:57:79:d5:42:76:e2:72:31:
         6c:c0:88:83:d3:0d:c7:20:1c:32:f3:4b:9d:43:b6:84:f4:99:
         8a:4e:1b:44:bc:7b:90:b8:04:9e:8c:d8:f4:43:43:d8:d0:20:
```

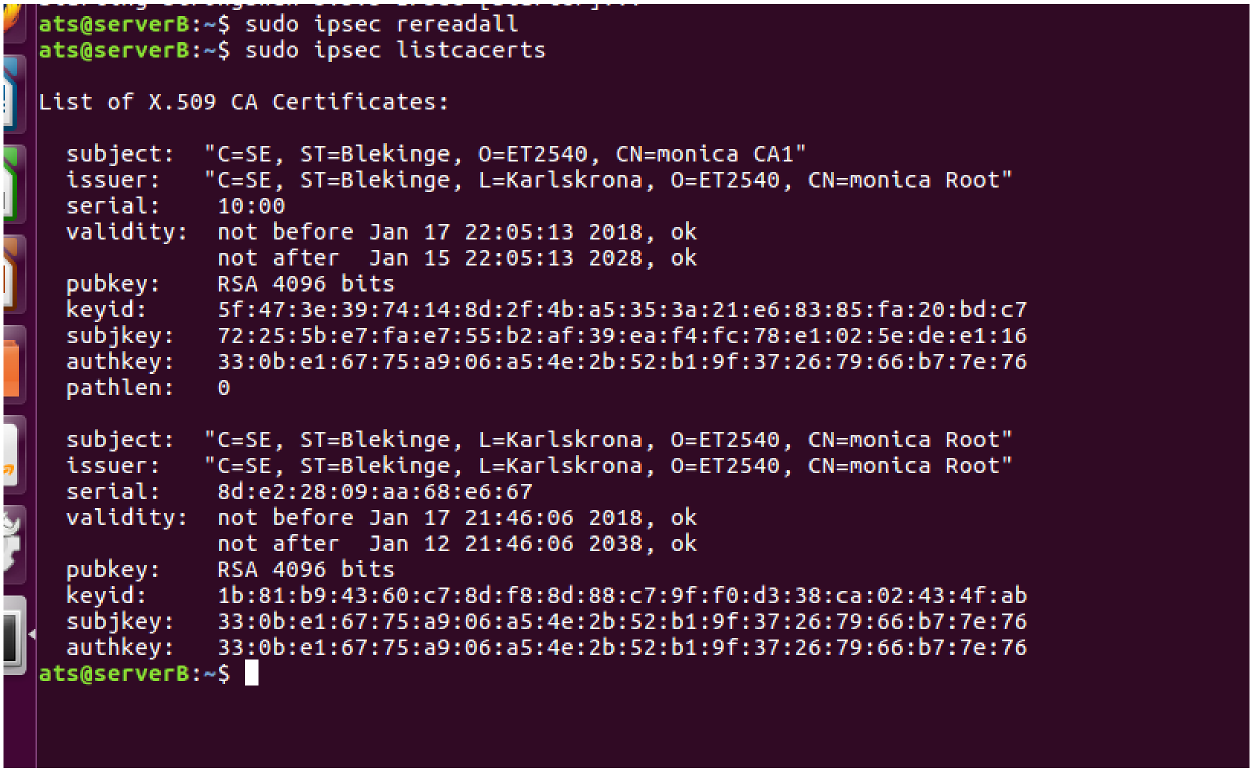
```
        bd:f4:a8:92:7f:ed:3c:13:13:2e:c5:81:c9:f8:39:d7:0e:44:
        91:fc:b4:40:34:c7:a7:de:d8:ef:5f:e0:df:6a:2f:db:f4:1d:
        65:0e:64:98:11:0f:db:82:52:79:ba:8d:27:90:6e:3d:e5:78:
        c8:27:19:ca:59:27:1d:8b:c7:9c:79:0e:06:e9:2d:65:6f:b5:
        6e:7a:57:c1:cd:89:45:88:08:49:bb:68:38:a4:f2:cf:f9:ff:
        e8:f8:49:4b:08:62:01:4a:55:25:50:ec:b5:aa:1b:c5:3b:52:
        e4:6a:11:43:70:76:4f:45:c7:3e:32:45:1c:45:94:3d:1d:70:
        47:52:ca:13:ff:31:d5:5f:87:47:ff:e9:48:27:c2:ad:1a:0a:
        e2:02:88:ce:30:00:d7:09:6b:90:89:d1:2b:bc:f0:f7:3e:92:
        75:39:b5:38:d1:5d:72:d6:8c:0b:48:f1:9a:c9:d1:d7:8d:8e:
        43:00:76:9b:8a:1a:4d:9e:4f:5a:ed:a9:52:ff:5d:03:9f:fb:
        7a:12:99:7f:ac:fe:08:47
```

```
ats@serverA:~/mota17_ca$ openssl ca -config ca1/openssl.cnf -
extensions server_cert -days 3650 -notext -in
ca1/csr/ca1.serverB.csr.pem -out ca1/certs/ca1.serverB.cert.pem
Using configuration from ca1/openssl.cnf
Enter pass phrase for
/home/ats/mota17_ca/ca1//private/ca1.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 8196 (0x2004)
        Validity
            Not Before: Jan 18 04:32:49 2018 GMT
            Not After : Jan 16 04:32:49 2028 GMT
        Subject:
            countryName               = SE
            stateOrProvinceName       = Blekinge
            localityName              = Karlskrona
            organizationName          = ET2540
            commonName                = 192.168.70.6
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:

CD:D6:39:20:92:D5:F3:73:70:7C:22:A3:46:5D:55:C0:96:06:F5:AE
            X509v3 Authority Key Identifier:

keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16

DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=monica Root
                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:
                  URI:https://localhost/ca1.crl.pem

Certificate is to be certified until Jan 16 04:32:49 2028 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
Data Base Updated


ats@serverA:~/mota17_ca$ openssl x509 -noout -text -in
ca1/certs/ca1.serverB.cert.pem
```

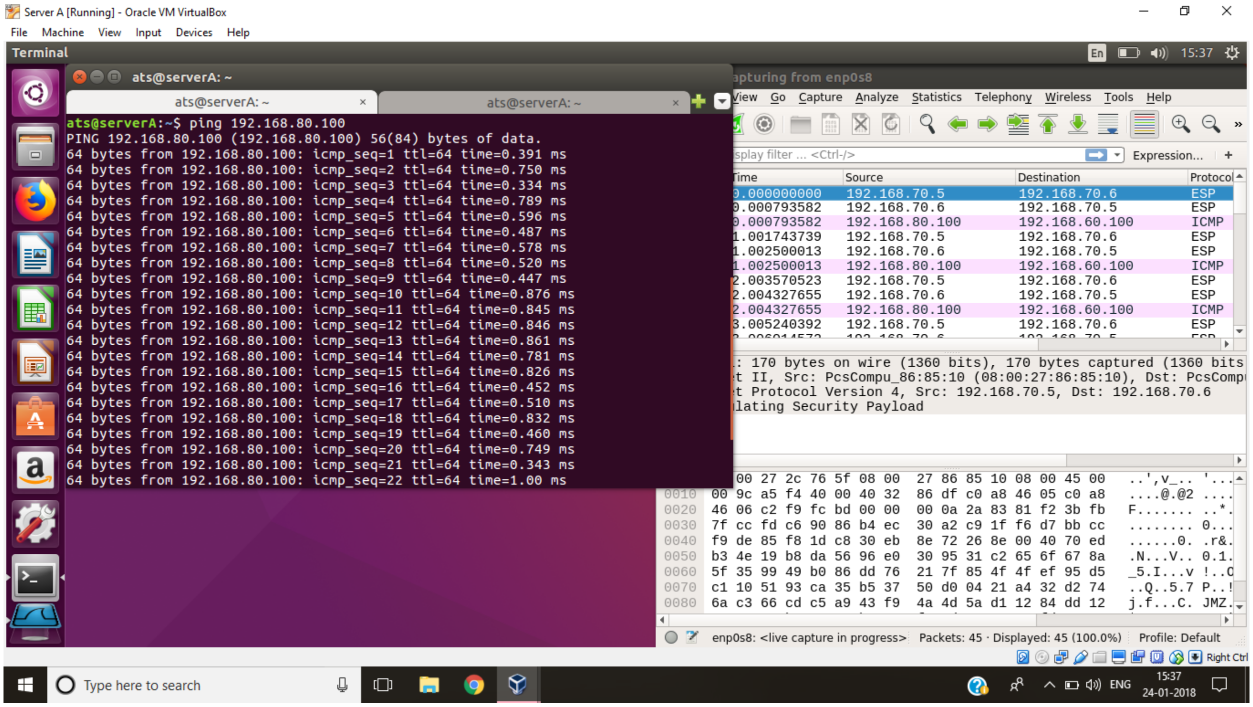
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8196 (0x2004)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=SE, ST=Blekinge, O=ET2540, CN=monica CA1
        Validity
            Not Before: Jan 18 04:32:49 2018 GMT
            Not After : Jan 16 04:32:49 2028 GMT
        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:c2:cc:96:dc:8b:24:04:c7:c4:9c:e3:41:c5:66:
                    f2:3a:c5:32:50:f5:12:22:b0:6b:af:5f:c6:35:c9:
                    55:a0:a2:7f:5d:96:d5:f4:a8:d0:ce:50:11:49:38:
                    57:56:54:ff:df:8a:57:33:24:10:a7:23:0a:10:40:
                    a7:96:2f:8b:11:35:2a:21:31:53:51:44:15:8a:fa:
                    1f:3f:58:0d:53:8a:bc:9f:1b:8d:9b:73:39:23:27:
                    3a:f8:e5:50:cb:1c:2f:fe:93:a1:b4:43:fa:0d:d6:
                    a6:d9:1e:13:cd:84:6b:7f:ef:a9:ca:53:62:bb:e8:
                    15:53:d9:78:19:0f:5d:6e:cc:06:fe:f9:b0:96:05:
                    fa:b6:ff:83:b1:6c:04:23:3c:de:e8:36:51:d1:26:
                    82:c2:da:9b:58:ac:6b:54:bd:fe:6d:ed:8e:1d:db:
                    01:e5:2a:48:7f:99:ed:ae:c7:18:ed:06:b9:b2:be:
                    5c:c9:74:ee:5f:9b:c0:5f:2a:52:3e:51:e5:45:fd:
                    81:63:ff:1a:fa:29:52:21:b8:c9:e3:72:9c:52:cb:
                    01:33:43:6b:a0:f3:ce:f2:d6:55:ee:bd:08:22:e7:
                    9d:f8:ad:a4:89:8b:32:80:69:4b:07:ee:7c:2e:5b:
                    e6:76:27:08:98:ae:92:be:99:2b:de:3c:23:74:ab:
                    ba:8b
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      X509v3 Subject Key Identifier:

CD:D6:39:20:92:D5:F3:73:70:7C:22:A3:46:5D:55:C0:96:06:F5:AE
      X509v3 Authority Key Identifier:

keyid:72:25:5B:E7:FA:E7:55:B2:AF:39:EA:F4:FC:78:E1:02:5E:DE:E1:16

DirName:/C=SE/ST=Blekinge/L=Karlskrona/O=ET2540/CN=monica Root
        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:
         URI:https://localhost/ca1.crl.pem

  Signature Algorithm: sha256WithRSAEncryption
     71:1f:9a:2d:2d:88:bb:5c:e4:95:3f:c5:4a:e6:b3:be:70:47:
     f6:7f:17:86:2b:8a:46:8a:8a:1e:35:4f:b5:f9:a4:cd:92:58:
     b9:01:db:fb:dd:51:91:94:e0:14:94:e7:6c:42:4e:c3:27:2a:
     66:dd:4a:a5:9b:3d:75:67:90:c9:3c:21:40:c4:14:c3:96:71:
     25:5c:7c:71:e9:81:dd:b3:d0:46:85:72:9d:6a:52:09:a2:6f:
     58:71:42:69:78:6b:58:9c:68:a2:26:86:09:83:2e:42:4e:c1:
     aa:5a:9a:c2:fe:9a:a7:ef:7a:f8:b2:4b:f2:23:c4:dd:77:aa:
     de:80:5e:c8:5e:ac:69:93:96:2c:f1:92:5c:8a:7a:19:04:c6:
     4a:5c:de:2c:a6:f8:16:79:f6:c9:29:21:38:57:81:e3:58:54:
```

```
    be:94:05:0f:c8:4a:0e:68:7e:85:75:81:7a:4e:e0:7f:0b:5f:
    23:ae:d9:c3:38:3c:46:e7:5c:db:19:2b:77:c9:45:2a:05:52:
    fb:c3:4c:fe:51:3f:8f:20:61:76:c1:dc:75:dd:65:9e:4a:e7:
    36:e7:62:27:d6:11:7e:ca:35:c3:90:b3:f1:ab:c0:42:de:02:
    76:95:fa:82:7c:b5:77:70:61:23:d2:d2:ce:96:82:e3:ba:d0:
    f6:9f:47:71:1a:a4:6c:ae:d2:97:8d:79:9a:76:d7:13:8e:26:
    26:44:49:89:ec:ea:f1:6e:81:e4:4b:06:f1:4b:fd:77:21:4e:
    9d:a8:7f:c6:c9:b4:4f:44:19:45:9e:00:fe:bc:5c:fa:f5:a1:
    08:a4:69:5f:bb:e7:06:c2:37:29:1a:fc:41:01:3e:80:50:d8:
    c7:95:7b:c3:d0:cd:ec:5b:7d:79:80:74:bb:9e:19:74:68:57:
    76:c8:af:a0:66:e6:0e:40:86:68:3c:3a:f6:88:26:97:a2:76:
    86:eb:79:14:2d:77:1a:dc:a8:e7:a5:86:53:c3:2a:be:a5:39:
    85:27:73:42:b8:ce:fc:0f:23:bc:1e:0a:85:85:79:71:86:53:
    49:57:cc:56:c4:cf:32:b0:53:81:63:21:6d:6c:f2:bb:29:d1:
    69:b2:fe:33:af:8e:b8:71:e9:37:4e:d5:f6:80:83:f6:dd:20:
    5d:54:6b:70:f8:f2:0b:16:fc:e5:3c:6f:09:f9:98:f7:7e:a9:
    e5:80:d3:43:88:4a:d5:7a:0e:d6:93:6d:0e:81:da:04:14:c4:
    8b:89:46:31:d7:fb:df:96:d6:07:44:26:0e:8f:08:94:f7:5f:
    b9:83:e9:1a:6e:1a:94:3e:7b:a7:0e:3d:7f:6c:01:11:74:6c:
    cc:be:fe:4d:dd:82:cc:5b
```

```
ats@serverA:~/mota17_ca$ openssl verify -CAfile certs/root.cert.pem -
untrusted ca1/certs/ca1.cert.pem ca1/certs/ca1.serverB.cert.pem
ca1/certs/ca1.serverB.cert.pem: OK
```



```
ats@serverB:~$ sudo ipsec rereadall
ats@serverB:~$ sudo ipsec listcacerts

List of X.509 CA Certificates:

  subject:  "C=SE, ST=Blekinge, O=ET2540, CN=monica CA1"
  issuer:   "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica Root"
  serial:    10:00
  validity:  not before Jan 17 22:05:13 2018, ok
             not after  Jan 15 22:05:13 2028, ok
  pubkey:    RSA 4096 bits
  keyid:     5f:47:3e:39:74:14:8d:2f:4b:a5:35:3a:21:e6:83:85:fa:20:bd:c7
  subjkey:   72:25:5b:e7:fa:e7:55:b2:af:39:ea:f4:fc:78:e1:02:5e:de:e1:16
  authkey:   33:0b:e1:67:75:a9:06:a5:4e:2b:52:b1:9f:37:26:79:66:b7:7e:76
  pathlen:   0

  subject:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica Root"
  issuer:   "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=monica Root"
  serial:    8d:e2:28:09:aa:68:e6:67
  validity:  not before Jan 17 21:46:06 2018, ok
             not after  Jan 12 21:46:06 2038, ok
  pubkey:    RSA 4096 bits
  keyid:     1b:81:b9:43:60:c7:8d:f8:8d:88:c7:9f:f0:d3:38:ca:02:43:4f:ab
  subjkey:   33:0b:e1:67:75:a9:06:a5:4e:2b:52:b1:9f:37:26:79:66:b7:7e:76
  authkey:   33:0b:e1:67:75:a9:06:a5:4e:2b:52:b1:9f:37:26:79:66:b7:7e:76
ats@serverB:~$ 
```


Server A [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En 15:37
ats@serverA: ~
ats@serverA: ~
ats@serverA: ~
apturing from enp0s8
View Go Capture Analyze Statistics Telephony Wireless Tools Help
splay filter ... <Ctrl-/>
Expression...
Right Ctrl
Type here to search
ENG 15:37 24-01-2018

```
ats@serverA:~$ ping 192.168.80.100
PING 192.168.80.100 (192.168.80.100) 56(84) bytes of data.
64 bytes from 192.168.80.100: icmp_seq=1 ttl=64 time=0.391 ms
64 bytes from 192.168.80.100: icmp_seq=2 ttl=64 time=0.750 ms
64 bytes from 192.168.80.100: icmp_seq=3 ttl=64 time=0.334 ms
64 bytes from 192.168.80.100: icmp_seq=4 ttl=64 time=0.789 ms
64 bytes from 192.168.80.100: icmp_seq=5 ttl=64 time=0.596 ms
64 bytes from 192.168.80.100: icmp_seq=6 ttl=64 time=0.487 ms
64 bytes from 192.168.80.100: icmp_seq=7 ttl=64 time=0.578 ms
64 bytes from 192.168.80.100: icmp_seq=8 ttl=64 time=0.520 ms
64 bytes from 192.168.80.100: icmp_seq=9 ttl=64 time=0.447 ms
64 bytes from 192.168.80.100: icmp_seq=10 ttl=64 time=0.876 ms
64 bytes from 192.168.80.100: icmp_seq=11 ttl=64 time=0.845 ms
64 bytes from 192.168.80.100: icmp_seq=12 ttl=64 time=0.846 ms
64 bytes from 192.168.80.100: icmp_seq=13 ttl=64 time=0.861 ms
64 bytes from 192.168.80.100: icmp_seq=14 ttl=64 time=0.781 ms
64 bytes from 192.168.80.100: icmp_seq=15 ttl=64 time=0.826 ms
64 bytes from 192.168.80.100: icmp_seq=16 ttl=64 time=0.452 ms
64 bytes from 192.168.80.100: icmp_seq=17 ttl=64 time=0.510 ms
64 bytes from 192.168.80.100: icmp_seq=18 ttl=64 time=0.832 ms
64 bytes from 192.168.80.100: icmp_seq=19 ttl=64 time=0.460 ms
64 bytes from 192.168.80.100: icmp_seq=20 ttl=64 time=0.749 ms
64 bytes from 192.168.80.100: icmp_seq=21 ttl=64 time=0.343 ms
64 bytes from 192.168.80.100: icmp_seq=22 ttl=64 time=1.00 ms
```

Time	Source	Destination	Protocol
0.000000000	192.168.70.5	192.168.70.6	ESP
0.000793582	192.168.70.6	192.168.70.5	ESP
0.000793582	192.168.80.100	192.168.60.100	ICMP
1.001743739	192.168.70.5	192.168.70.6	ESP
1.002500013	192.168.70.6	192.168.70.5	ESP
1.002500013	192.168.80.100	192.168.60.100	ICMP
2.003570523	192.168.70.5	192.168.70.6	ESP
2.004327655	192.168.70.6	192.168.70.5	ESP
2.004327655	192.168.80.100	192.168.60.100	ICMP
3.005240392	192.168.70.5	192.168.70.6	ESP

```
: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits
t II, Src: PcsCompu_86:85:10 (08:00:27:86:85:10), Dst: PcsCompu
t Protocol Version 4, Src: 192.168.70.5, Dst: 192.168.70.6
lating Security Payload
```

```
     00 27 2c 76 5f 08 00  27 86 85 10 08 00 45 00   ..',v_.. '...
0010 00 9c a5 f4 40 00 40 32  86 df c0 a8 46 05 c0 a8   ....@.@2 ....
0020 46 06 c2 f9 fc bd 00 00  00 0a 2a 83 81 f2 3b fb   F....... ..*.
0030 7f cc fd c6 90 86 b4 ec  30 a2 c9 1f f6 d7 bb cc   ........ 0...
0040 f9 de 85 f8 1d c8 30 eb  8e 72 26 8e 00 40 70 ed   ......0. .r&.
0050 b3 4e 19 b8 da 56 96 e0  30 95 31 c2 65 6f 67 8a   .N...V.. 0.1.
0060 5f 35 99 49 b0 86 dd 76  21 7f 85 4f 4f ef 95 d5   _5.I...v !..O
0070 c1 10 51 93 ca 35 b5 37  50 d0 04 21 a4 32 d2 74   ..Q..5.7 P..!
0080 6a c3 66 cd c5 a9 43 f9  4a 4d 5a d1 12 84 dd 12   j.f...C. JMZ.
```

enp0s8: <live capture in progress> Packets: 45 · Displayed: 45 (100.0%) Profile: Default

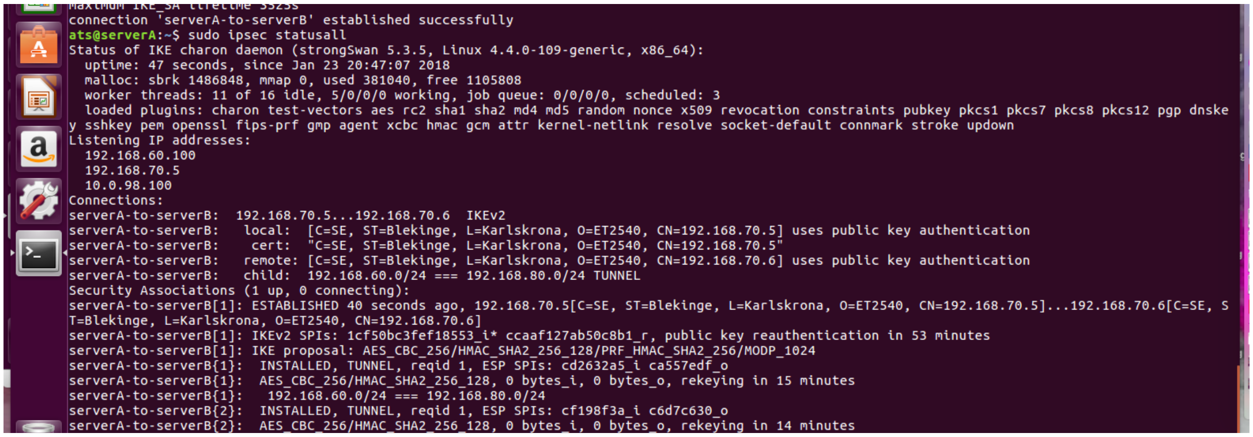
Task 19: Tunnel mode VPN with cert authentication between Server A and Server B

: **ServerA**

```
ats@serverA:~$ sudo cat /etc/ipsec.secrets
[sudo] password for ats:
# 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.

: RSA /etc/ipsec.d/private/ca1.serverA.key.pem"
ats@serverA:~$

sudo cat ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
        charondebug="all"
        strictcrlpolicy=no
        uniqueids=yes

# Add connections here.

conn %default
        ikelifetime=60m
        keylife=20m
        rekeymargin=3m
        keyingtries=1
        keyexchange=ikev2
#       authby=secret
```

```
        mobike=no

conn serverA-to-serverB

        left=192.168.70.5
        leftsubnet=192.168.60.0/24
        leftcert=/etc/ipsec.d/cacerts/ca1.serverA.cert.pem
        leftfirewall=yes
        leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
        rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
        right=192.168.70.6
        rightsubnet=192.168.80.0/24
        ike=aes256-sha2_256-modp1024!
        esp=aes256-sha2_256!
        auto=add
        type=tunnel




# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#      leftsubnet=10.1.0.0/16
#      leftcert=selfCert.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=myCert.pem
#	right=192.168.0.2
#	rightsubnet=10.2.0.0/16
#	rightid="C=CH, O=Linux strongSwan CN=peer name"
#	auto=start
```

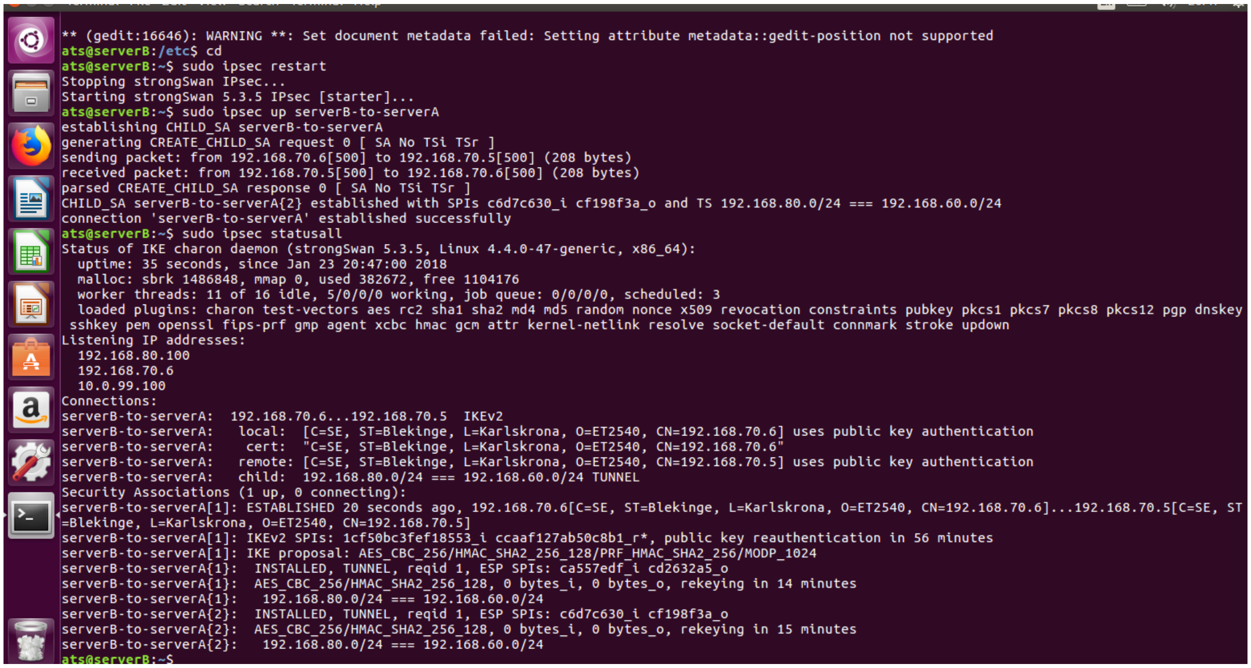


```
maximum IKE_SA lifetime 3323s
connection 'serverA-to-serverB' established successfully
ats@serverA:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-109-generic, x86_64):
  uptime: 47 seconds, since Jan 23 20:47:07 2018
  malloc: sbrk 1486848, mmap 0, used 381040, free 1105808
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnske
y sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB:  192.168.70.5...192.168.70.6  IKEv2
serverA-to-serverB:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverA-to-serverB:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
serverA-to-serverB:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverA-to-serverB:   child:  192.168.60.0/24 === 192.168.80.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
serverA-to-serverB[1]: ESTABLISHED 40 seconds ago, 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE, S
T=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
serverA-to-serverB[1]: IKEv2 SPIs: 1cf50bc3fef18553_i* ccaaf127ab50c8b1_r, public key reauthentication in 53 minutes
serverA-to-serverB[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
serverA-to-serverB{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cd2632a5_i ca557edf_o
serverA-to-serverB{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
serverA-to-serverB{1}:   192.168.60.0/24 === 192.168.80.0/24
serverA-to-serverB{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cf198f3a_i c6d7c630_o
serverA-to-serverB{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes
```

Server B

```
ats@serverB:/etc$ sudo cat ipsec.conf
# ipsec.conf - strongSwan IPsec configuration file

# basic configuration

config setup
			strictcrlpolicy=no
			uniqueids=yes
			charondebug="all"

# Add connections here.

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

conn serverB-to-serverA
			left=192.168.70.6
			leftsubnet=192.168.80.0/24
			leftfirewall=yes
			leftcert=/etc/ipsec.d/cacerts/ca1.serverB.cert.pem
			leftid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.6"
			rightid="C=SE, ST=Blekinge, L=Karlskrona, O=ET2540,
CN=192.168.70.5"
			right=192.168.70.5
			rightsubnet=192.168.60.0/24
			ike=aes256-sha2_256-modp1024!
			esp=aes256-sha2_256!
			auto=add
			type=tunnel



			# Sample VPN connections
```

```
#conn sample-self-signed
#	leftsubnet=10.1.0.0/16
#	leftcert=selfCert.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=myCert.pem
#	right=192.168.0.2
#	rightsubnet=10.2.0.0/16
#	rightid="C=CH, O=Linux strongSwan CN=peer name"
#	auto=start
ats@serverB:/etc$
```



```
** (gedit:16646): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
ats@serverB:/etc$ cd
ats@serverB:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.3.5 IPsec [starter]...
ats@serverB:~$ sudo ipsec up serverB-to-serverA
establishing CHILD_SA serverB-to-serverA
generating CREATE_CHILD_SA request 0 [ SA No TSi TSr ]
sending packet: from 192.168.70.6[500] to 192.168.70.5[500] (208 bytes)
received packet: from 192.168.70.5[500] to 192.168.70.6[500] (208 bytes)
parsed CREATE_CHILD_SA response 0 [ SA No TSi TSr ]
CHILD_SA serverB-to-serverA{2} established with SPIs c6d7c630_i cf198f3a_o and TS 192.168.80.0/24 === 192.168.60.0/24
connection 'serverB-to-serverA' established successfully
ats@serverB:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-47-generic, x86_64):
  uptime: 35 seconds, since Jan 23 20:47:00 2018
  malloc: sbrk 1486848, mmap 0, used 382672, free 1104176
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey
 sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA:  192.168.70.6...192.168.70.5  IKEv2
serverB-to-serverA:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA:   child:  192.168.80.0/24 === 192.168.60.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
serverB-to-serverA[1]: ESTABLISHED 20 seconds 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[1]: IKEv2 SPIs: 1cf50bc3fef18553_i ccaaf127ab50c8b1_r*, public key reauthentication in 56 minutes
serverB-to-serverA[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
serverB-to-serverA{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca557edf_i cd2632a5_o
serverB-to-serverA{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes
serverB-to-serverA{1}:   192.168.80.0/24 === 192.168.60.0/24
serverB-to-serverA{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6d7c630_i cf198f3a_o
serverB-to-serverA{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
serverB-to-serverA{2}:   192.168.80.0/24 === 192.168.60.0/24
ats@serverB:~$
```

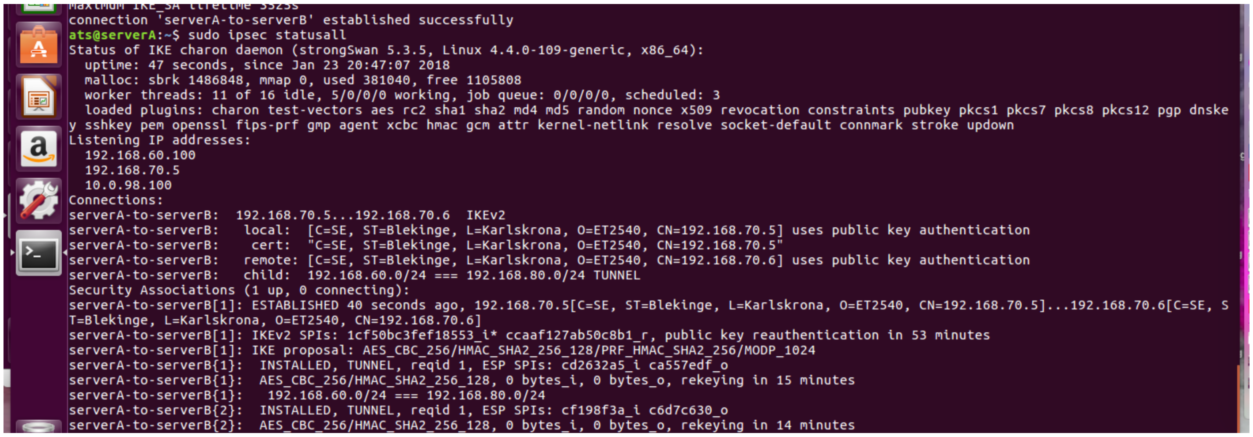
Task 20: Tunnel mode VPN with IP forwarding for client A and client B

In order to do ip forwarding from client A to Client B we need to use the following commands up the ipsec connection from server A to server B to enable ip forwarding between client A to client B.

Sudo ipsec up serverA-to-serverB.

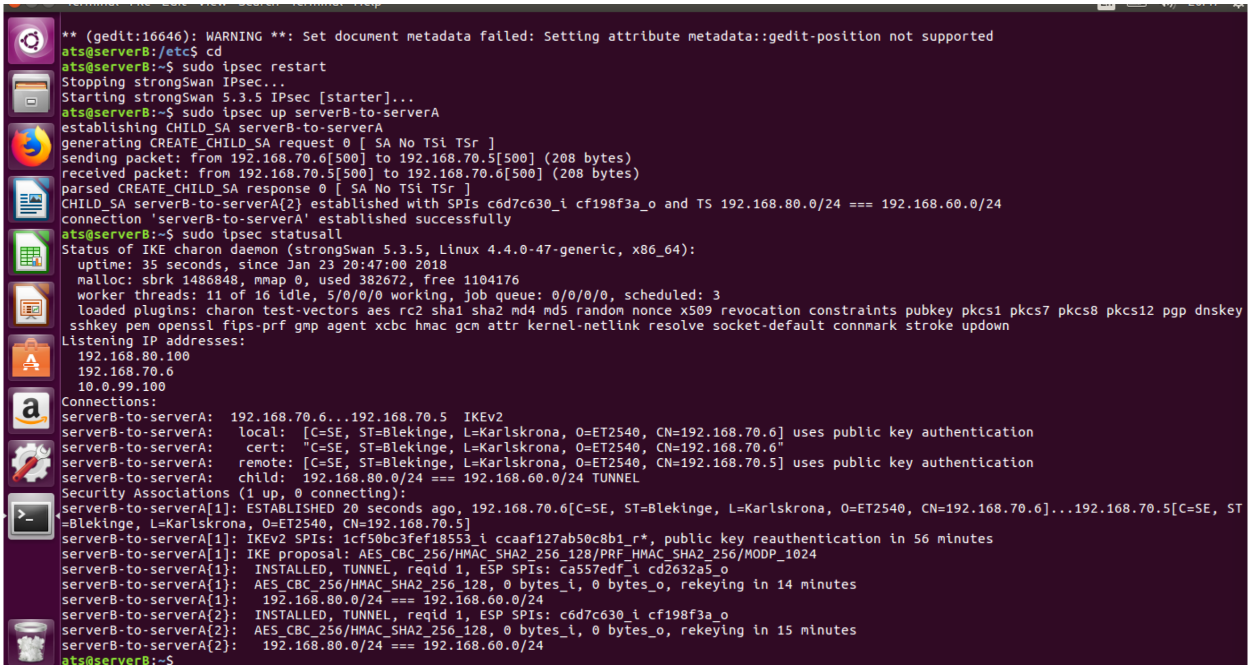
Sudo ipsec statusall.

Server A

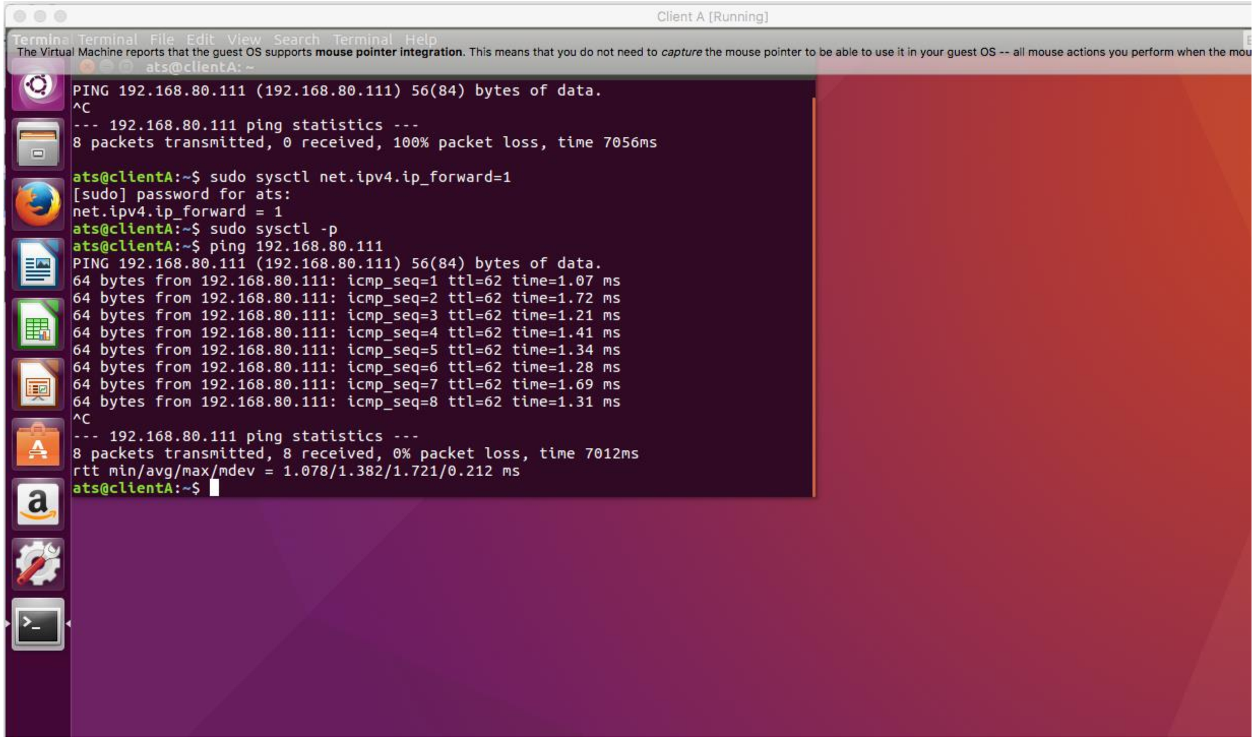


```
maximum IKE_SA lifetime 3325s
connection 'serverA-to-serverB' established successfully
ats@serverA:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-109-generic, x86_64):
  uptime: 47 seconds, since Jan 23 20:47:07 2018
  malloc: sbrk 1486848, mmap 0, used 381040, free 1105808
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnske
y sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB:  192.168.70.5...192.168.70.6  IKEv2
serverA-to-serverB:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverA-to-serverB:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
serverA-to-serverB:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverA-to-serverB:   child:  192.168.60.0/24 === 192.168.80.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
serverA-to-serverB[1]: ESTABLISHED 40 seconds ago, 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE, S
T=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
serverA-to-serverB[1]: IKEv2 SPIs: 1cf50bc3fef18553_i* ccaaf127ab50c8b1_r, public key reauthentication in 53 minutes
serverA-to-serverB[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
serverA-to-serverB{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cd2632a5_i ca557edf_o
serverA-to-serverB{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
serverA-to-serverB{1}:   192.168.60.0/24 === 192.168.80.0/24
serverA-to-serverB{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cf198f3a_i c6d7c630_o
serverA-to-serverB{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes
```

Server B:

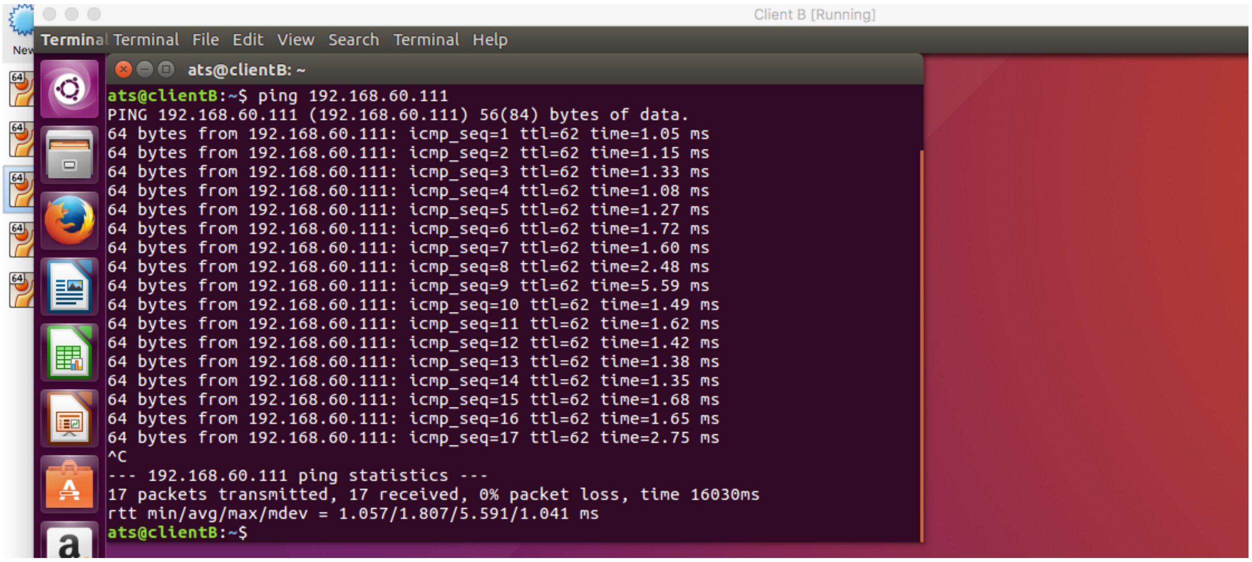


```
** (gedit:16646): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
ats@serverB:/etc$ cd
ats@serverB:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.3.5 IPsec [starter]...
ats@serverB:~$ sudo ipsec up serverB-to-serverA
establishing CHILD_SA serverB-to-serverA
generating CREATE_CHILD_SA request 0 [ SA No TSi TSr ]
sending packet: from 192.168.70.6[500] to 192.168.70.5[500] (208 bytes)
received packet: from 192.168.70.5[500] to 192.168.70.6[500] (208 bytes)
parsed CREATE_CHILD_SA response 0 [ SA No TSi TSr ]
CHILD_SA serverB-to-serverA{2} established with SPIs c6d7c630_i cf198f3a_o and TS 192.168.80.0/24 === 192.168.60.0/24
connection 'serverB-to-serverA' established successfully
ats@serverB:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-47-generic, x86_64):
  uptime: 35 seconds, since Jan 23 20:47:00 2018
  malloc: sbrk 1486848, mmap 0, used 382672, free 1104176
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey
 sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA:  192.168.70.6...192.168.70.5  IKEv2
serverB-to-serverA:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA:   child:  192.168.80.0/24 === 192.168.60.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
serverB-to-serverA[1]: ESTABLISHED 20 seconds 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[1]: IKEv2 SPIs: 1cf50bc3fef18553_i ccaaf127ab50c8b1_r*, public key reauthentication in 56 minutes
serverB-to-serverA[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
serverB-to-serverA{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca557edf_i cd2632a5_o
serverB-to-serverA{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes
serverB-to-serverA{1}:   192.168.80.0/24 === 192.168.60.0/24
serverB-to-serverA{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6d7c630_i cf198f3a_o
serverB-to-serverA{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
serverB-to-serverA{2}:   192.168.80.0/24 === 192.168.60.0/24
ats@serverB:~$
```



The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that you do not need to *capture* the mouse pointer to be able to use it in your guest OS -- all mouse actions you perform when the mou

```
PING 192.168.80.111 (192.168.80.111) 56(84) bytes of data.
^C
--- 192.168.80.111 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7056ms

ats@clientA:~$ sudo sysctl net.ipv4.ip_forward=1
[sudo] password for ats:
net.ipv4.ip_forward = 1
ats@clientA:~$ sudo sysctl -p
ats@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=1.07 ms
64 bytes from 192.168.80.111: icmp_seq=2 ttl=62 time=1.72 ms
64 bytes from 192.168.80.111: icmp_seq=3 ttl=62 time=1.21 ms
64 bytes from 192.168.80.111: icmp_seq=4 ttl=62 time=1.41 ms
64 bytes from 192.168.80.111: icmp_seq=5 ttl=62 time=1.34 ms
64 bytes from 192.168.80.111: icmp_seq=6 ttl=62 time=1.28 ms
64 bytes from 192.168.80.111: icmp_seq=7 ttl=62 time=1.69 ms
64 bytes from 192.168.80.111: icmp_seq=8 ttl=62 time=1.31 ms
^C
--- 192.168.80.111 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7012ms
rtt min/avg/max/mdev = 1.078/1.382/1.721/0.212 ms
ats@clientA:~$
```



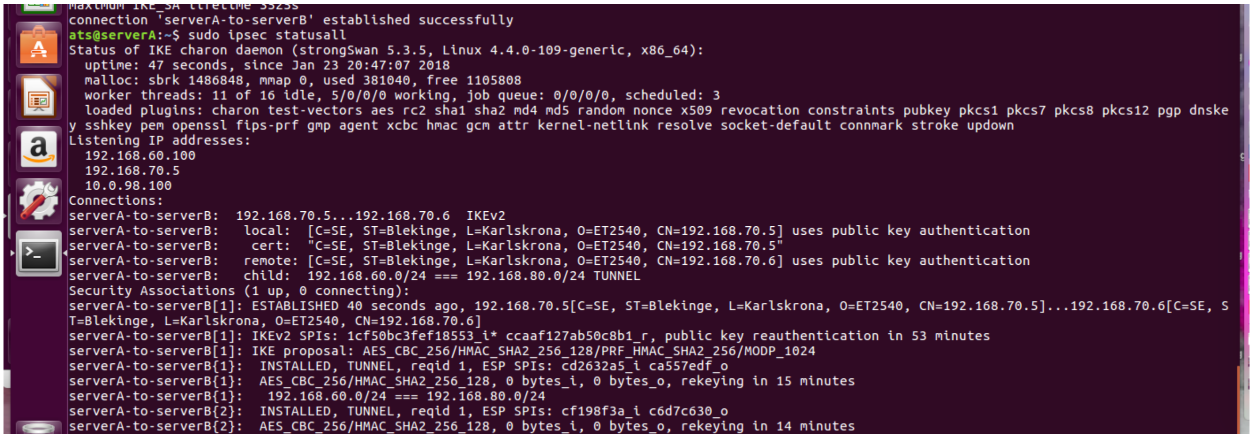
```
ats@clientB:~$ ping 192.168.60.111
PING 192.168.60.111 (192.168.60.111) 56(84) bytes of data.
64 bytes from 192.168.60.111: icmp_seq=1 ttl=62 time=1.05 ms
64 bytes from 192.168.60.111: icmp_seq=2 ttl=62 time=1.15 ms
64 bytes from 192.168.60.111: icmp_seq=3 ttl=62 time=1.33 ms
64 bytes from 192.168.60.111: icmp_seq=4 ttl=62 time=1.08 ms
64 bytes from 192.168.60.111: icmp_seq=5 ttl=62 time=1.27 ms
64 bytes from 192.168.60.111: icmp_seq=6 ttl=62 time=1.72 ms
64 bytes from 192.168.60.111: icmp_seq=7 ttl=62 time=1.60 ms
64 bytes from 192.168.60.111: icmp_seq=8 ttl=62 time=2.48 ms
64 bytes from 192.168.60.111: icmp_seq=9 ttl=62 time=5.59 ms
64 bytes from 192.168.60.111: icmp_seq=10 ttl=62 time=1.49 ms
64 bytes from 192.168.60.111: icmp_seq=11 ttl=62 time=1.62 ms
64 bytes from 192.168.60.111: icmp_seq=12 ttl=62 time=1.42 ms
64 bytes from 192.168.60.111: icmp_seq=13 ttl=62 time=1.38 ms
64 bytes from 192.168.60.111: icmp_seq=14 ttl=62 time=1.35 ms
64 bytes from 192.168.60.111: icmp_seq=15 ttl=62 time=1.68 ms
64 bytes from 192.168.60.111: icmp_seq=16 ttl=62 time=1.65 ms
64 bytes from 192.168.60.111: icmp_seq=17 ttl=62 time=2.75 ms
^C
--- 192.168.60.111 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16030ms
rtt min/avg/max/mdev = 1.057/1.807/5.591/1.041 ms
ats@clientB:~$
```

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

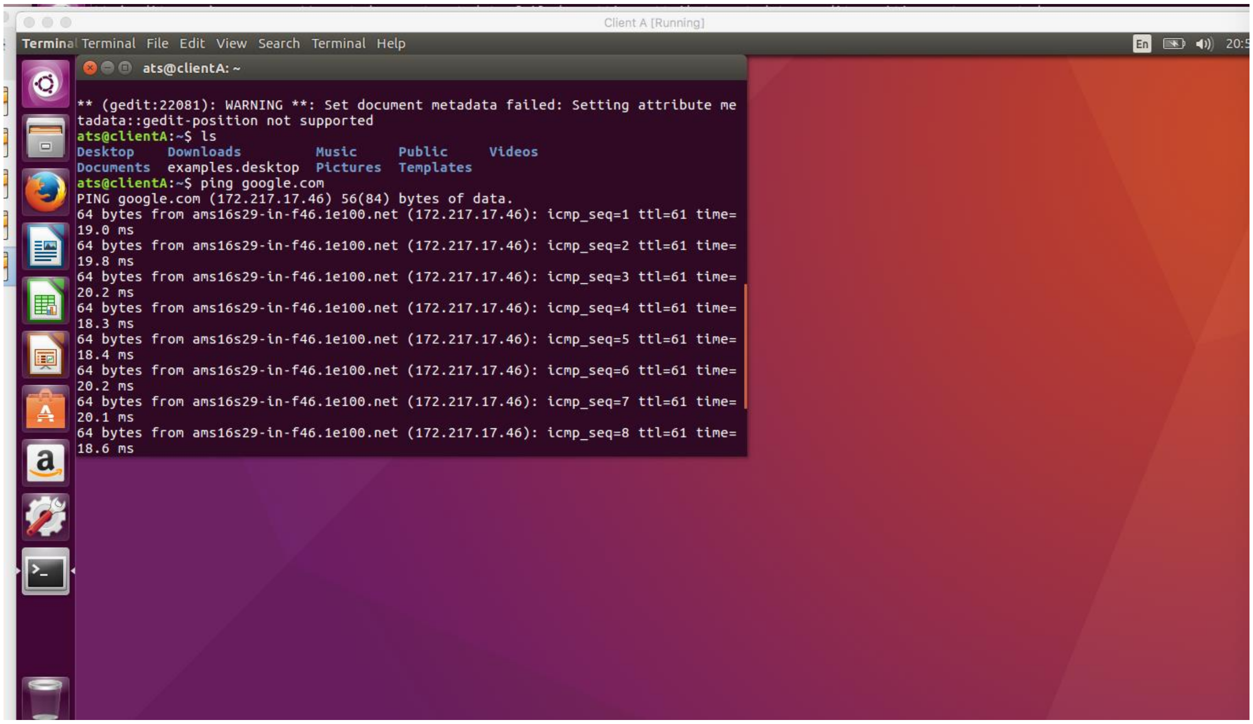
Client A

To enable default Drop firewall rules in server B copy the firewall.sh file from server A to server B, and enable the default firewall rules in firewall.sh.
./firewall.sh

Server A

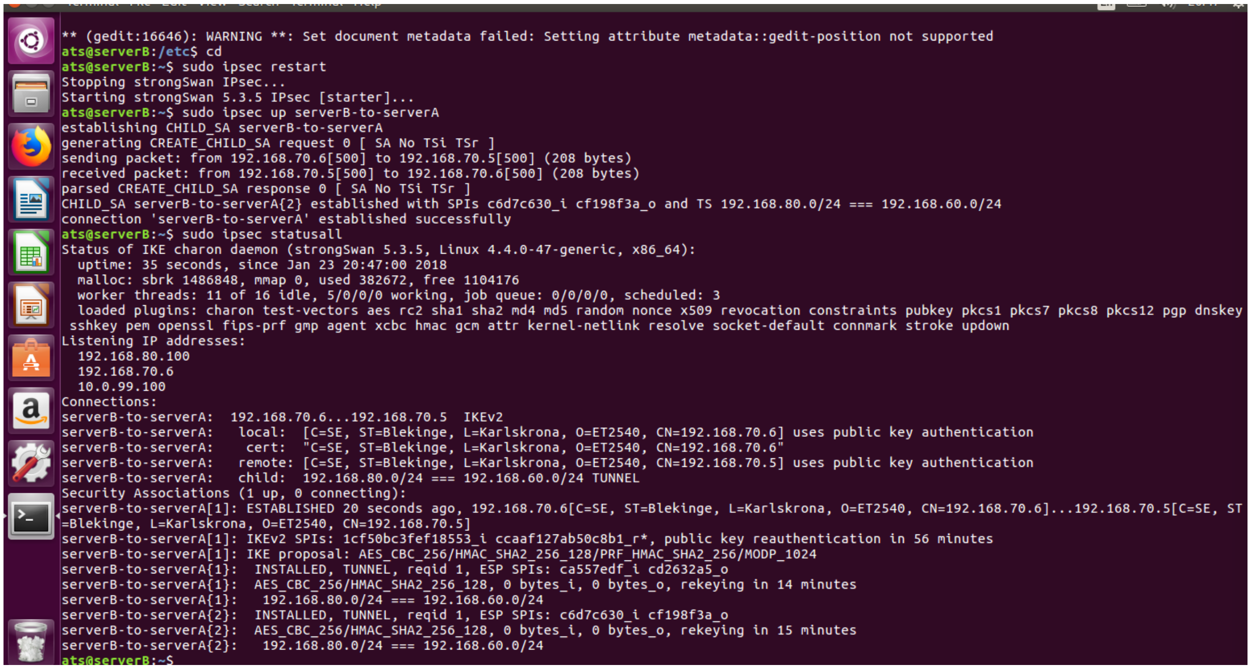


```
maximum IKE_SA lifetime 3325s
connection 'serverA-to-serverB' established successfully
ats@serverA:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-109-generic, x86_64):
  uptime: 47 seconds, since Jan 23 20:47:07 2018
  malloc: sbrk 1486848, mmap 0, used 381040, free 1105808
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnske
y sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.60.100
  192.168.70.5
  10.0.98.100
Connections:
serverA-to-serverB:  192.168.70.5...192.168.70.6  IKEv2
serverA-to-serverB:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverA-to-serverB:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5"
serverA-to-serverB:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverA-to-serverB:   child:  192.168.60.0/24 === 192.168.80.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
serverA-to-serverB[1]: ESTABLISHED 40 seconds ago, 192.168.70.5[C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5]...192.168.70.6[C=SE, S
T=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6]
serverA-to-serverB[1]: IKEv2 SPIs: 1cf50bc3fef18553_i* ccaaf127ab50c8b1_r, public key reauthentication in 53 minutes
serverA-to-serverB[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
serverA-to-serverB{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cd2632a5_i ca557edf_o
serverA-to-serverB{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
serverA-to-serverB{1}:   192.168.60.0/24 === 192.168.80.0/24
serverA-to-serverB{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cf198f3a_i c6d7c630_o
serverA-to-serverB{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes
```

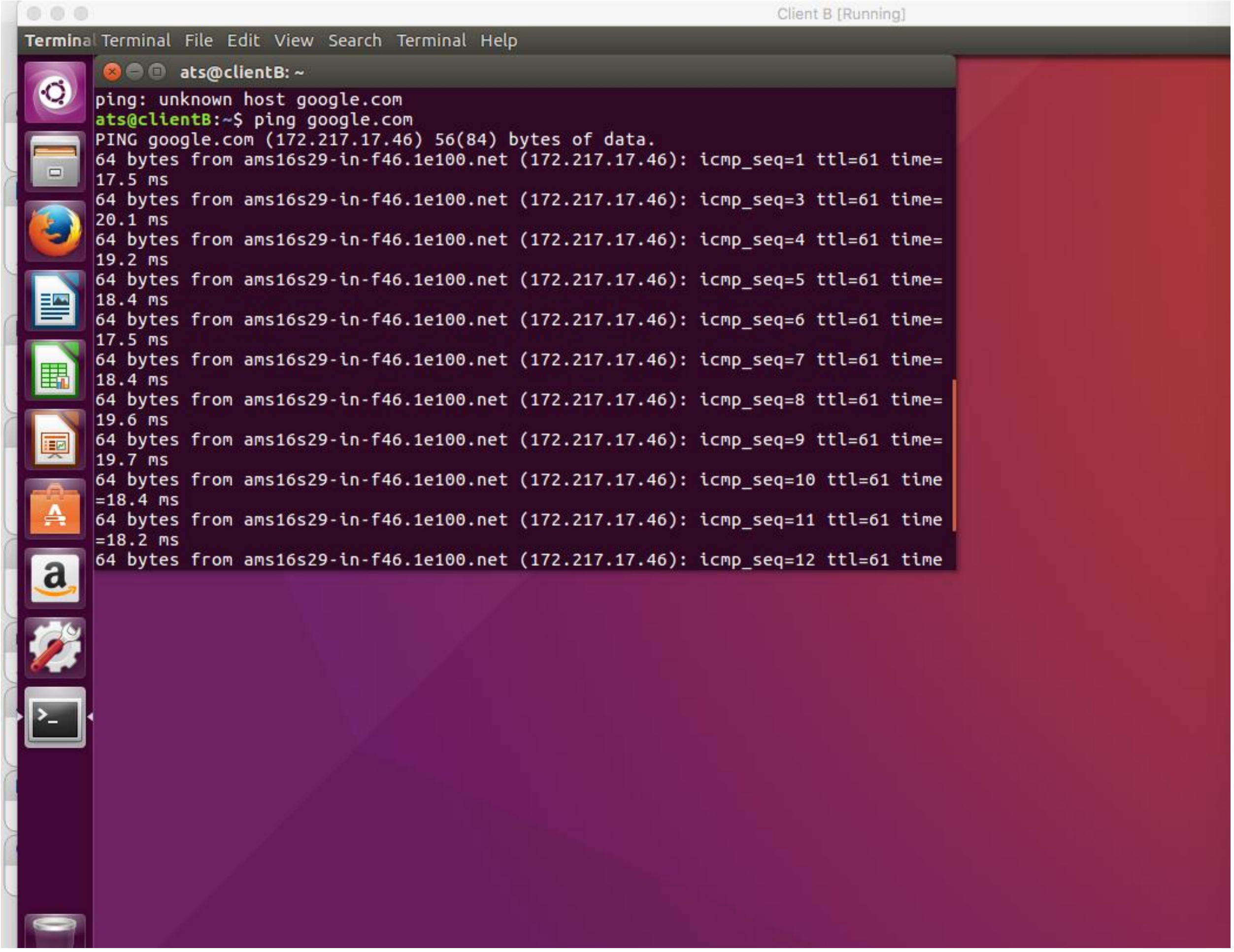


```
** (gedit:22081): WARNING **: Set document metadata failed: Setting attribute me
tadata::gedit-position not supported
ats@clientA:~$ ls
Desktop    Downloads         Music     Public     Videos
Documents  examples.desktop  Pictures  Templates
ats@clientA:~$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data.
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=1 ttl=61 time=
19.0 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=2 ttl=61 time=
19.8 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=3 ttl=61 time=
20.2 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=4 ttl=61 time=
18.3 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=5 ttl=61 time=
18.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=6 ttl=61 time=
20.2 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=7 ttl=61 time=
20.1 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=8 ttl=61 time=
18.6 ms
```

Server B



```
** (gedit:16646): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
ats@serverB:/etc$ cd
ats@serverB:~$ sudo ipsec restart
Stopping strongSwan IPsec...
Starting strongSwan 5.3.5 IPsec [starter]...
ats@serverB:~$ sudo ipsec up serverB-to-serverA
establishing CHILD_SA serverB-to-serverA
generating CREATE_CHILD_SA request 0 [ SA No TSi TSr ]
sending packet: from 192.168.70.6[500] to 192.168.70.5[500] (208 bytes)
received packet: from 192.168.70.5[500] to 192.168.70.6[500] (208 bytes)
parsed CREATE_CHILD_SA response 0 [ SA No TSi TSr ]
CHILD_SA serverB-to-serverA{2} established with SPIs c6d7c630_i cf198f3a_o and TS 192.168.80.0/24 === 192.168.60.0/24
connection 'serverB-to-serverA' established successfully
ats@serverB:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-47-generic, x86_64):
  uptime: 35 seconds, since Jan 23 20:47:00 2018
  malloc: sbrk 1486848, mmap 0, used 382672, free 1104176
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
  loaded plugins: charon test-vectors aes rc2 sha1 sha2 md4 md5 random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey
 sshkey pem openssl fips-prf gmp agent xcbc hmac gcm attr kernel-netlink resolve socket-default connmark stroke updown
Listening IP addresses:
  192.168.80.100
  192.168.70.6
  10.0.99.100
Connections:
serverB-to-serverA:  192.168.70.6...192.168.70.5  IKEv2
serverB-to-serverA:   local:  [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6] uses public key authentication
serverB-to-serverA:    cert:  "C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.6"
serverB-to-serverA:   remote: [C=SE, ST=Blekinge, L=Karlskrona, O=ET2540, CN=192.168.70.5] uses public key authentication
serverB-to-serverA:   child:  192.168.80.0/24 === 192.168.60.0/24 TUNNEL
Security Associations (1 up, 0 connecting):
serverB-to-serverA[1]: ESTABLISHED 20 seconds 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[1]: IKEv2 SPIs: 1cf50bc3fef18553_i ccaaf127ab50c8b1_r*, public key reauthentication in 56 minutes
serverB-to-serverA[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
serverB-to-serverA{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: ca557edf_i cd2632a5_o
serverB-to-serverA{1}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes
serverB-to-serverA{1}:   192.168.80.0/24 === 192.168.60.0/24
serverB-to-serverA{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6d7c630_i cf198f3a_o
serverB-to-serverA{2}:  AES_CBC_256/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 15 minutes
serverB-to-serverA{2}:   192.168.80.0/24 === 192.168.60.0/24
ats@serverB:~$
```



```
ping: unknown host google.com
ats@clientB:~$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data.
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=1 ttl=61 time=
17.5 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=3 ttl=61 time=
20.1 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=4 ttl=61 time=
19.2 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=5 ttl=61 time=
18.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=6 ttl=61 time=
17.5 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=7 ttl=61 time=
18.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=8 ttl=61 time=
19.6 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=9 ttl=61 time=
19.7 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=10 ttl=61 time
=18.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=11 ttl=61 time
=18.2 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=12 ttl=61 time
```