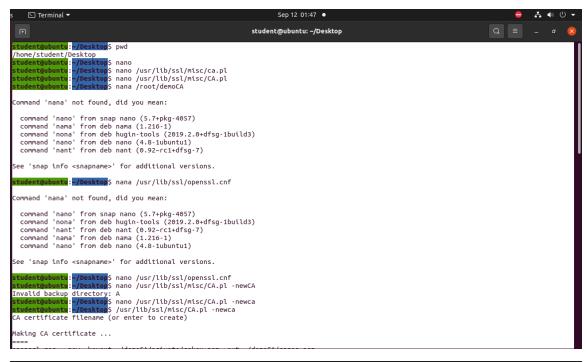
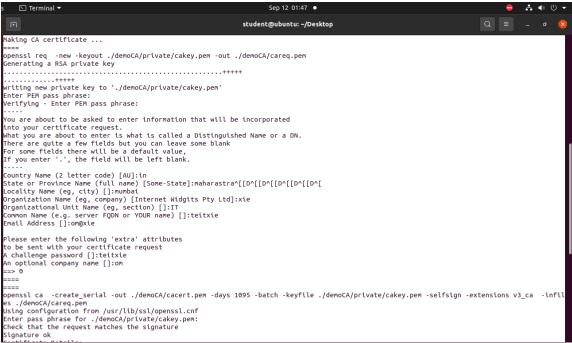
```
Q I
                               student@ubuntu: ~/Desktop
  GNU nano 4.8
                               /usr/lib/ssl/misc/CA.pl
!/usr/bin/perl
# Wrapper around the ca to make it easier to use
use strict;
use warnings;
ny $openssl = "openssl":
Lf(
    leftned $ENV{'OPENSSL'}) {
    $openssl = $ENV{'OPENSSL'};
                [ File '/usr/lib/ssl/misc/CA.pl' is unwritable ]
             ^O Write Out ^W Where Is ^K Cut Text ^J Justify
                                                                    ^C Cur Pos
             ^R Read File ^\ Replace
                                         ^U Paste Text^T To Spell
^X Exit
                                                                       Go To Line
                               student@ubuntu: ~/Desktop
                                                               Q
Invalid backup directory: A
student@ubuntu:~/Desktop$ nano /usr/lib/ssl/misc/CA.pl -newca
student@ubuntu:~/Desktop$ /usr/lib/ssl/misc/CA.pl -newca
CA certificate filename (or enter to create)
Making CA certificate ...
openssl req -new -keyout ./demoCA/private/cakey.pem -out ./demoCA/careq.pem
Generating a RSA private key
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
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,
```

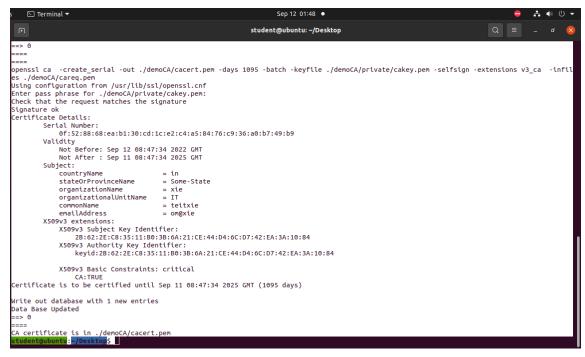
If you enter '.', the field will be left blank.

State or Province Name (full name) [Some-State]:maharastra

Country Name (2 letter code) [AU]:in







```
Sep 12 01:51 •
                                                                                                                                                                                                                          A •
                                                                                       student@ubuntu: ~/Desktop/demoCA/newcerts
                                                                                                                                                                                                        Q = _ ø
  => O
====
openssl ca -create_serial -out ./demoCA/cacert.pem -days 1095 -batch -keyfile ./demoCA/private/cakey.pem -selfsign -extensions v3_ca -infil
es ./demoCA/careq.pem
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
  Not After : Sep 11 00.

Subject:
countryName
stateOrProvinceName
organizationName
organizationalUnitName
                                                              = in
= Some-State
= xie
= IT
                                                              = teitxie
= om@xie
                   commonName
emailAddress
             X509v3 extensions:
                   X599V3 Schelatons.
X599V3 Subject Key Identifier:
28:62:2E:68:35:11:88:38:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
X509V3 Authority Key Identifier:
keyid:2B:62:2E:C8:35:11:80:38:6A:21:CE:44:D4:6C:D7:42:EA:3A:10:84
                   X509v3 Basic Constraints: critical
CA:TRUE
Certificate is to be certified until Sep 11 08:47:34 2025 GMT (1095 days)
Write out database with 1 new entries
Data Base Updated
==> 0
CA certificate is in ./demoCA/cacert.pem
student@ubuntu:~/Desktop$ cd demoCA/newcerts
```

