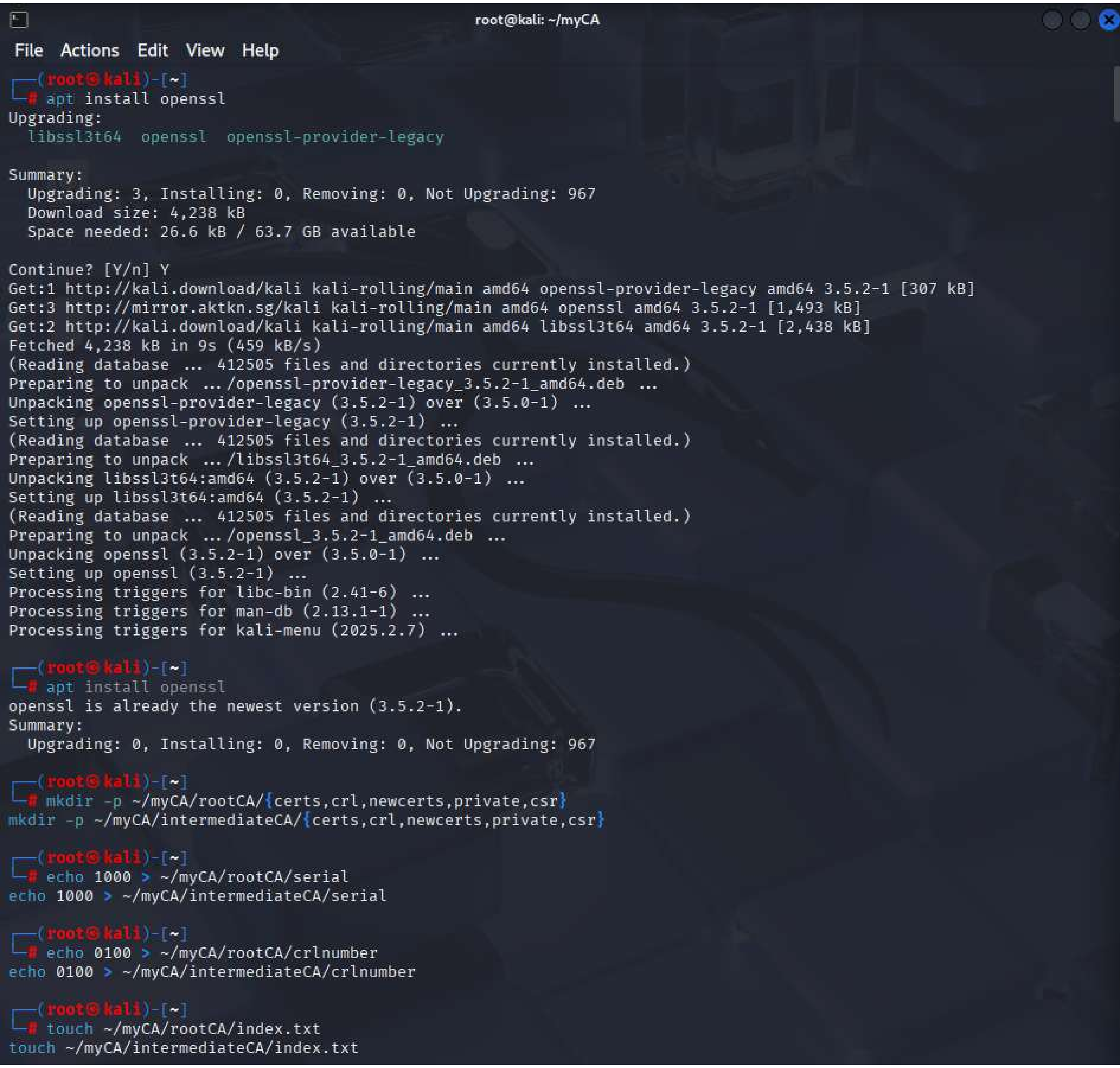
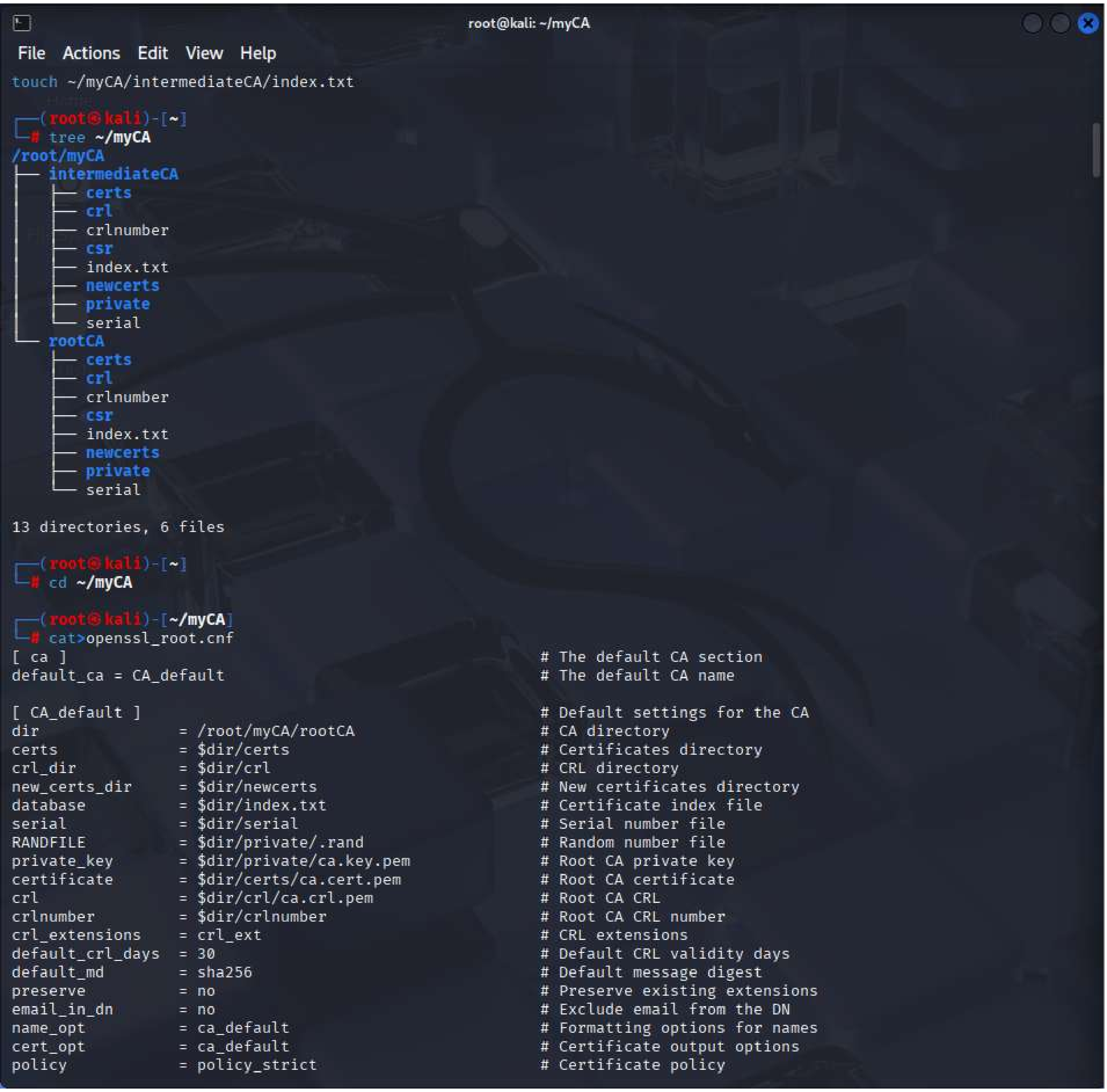
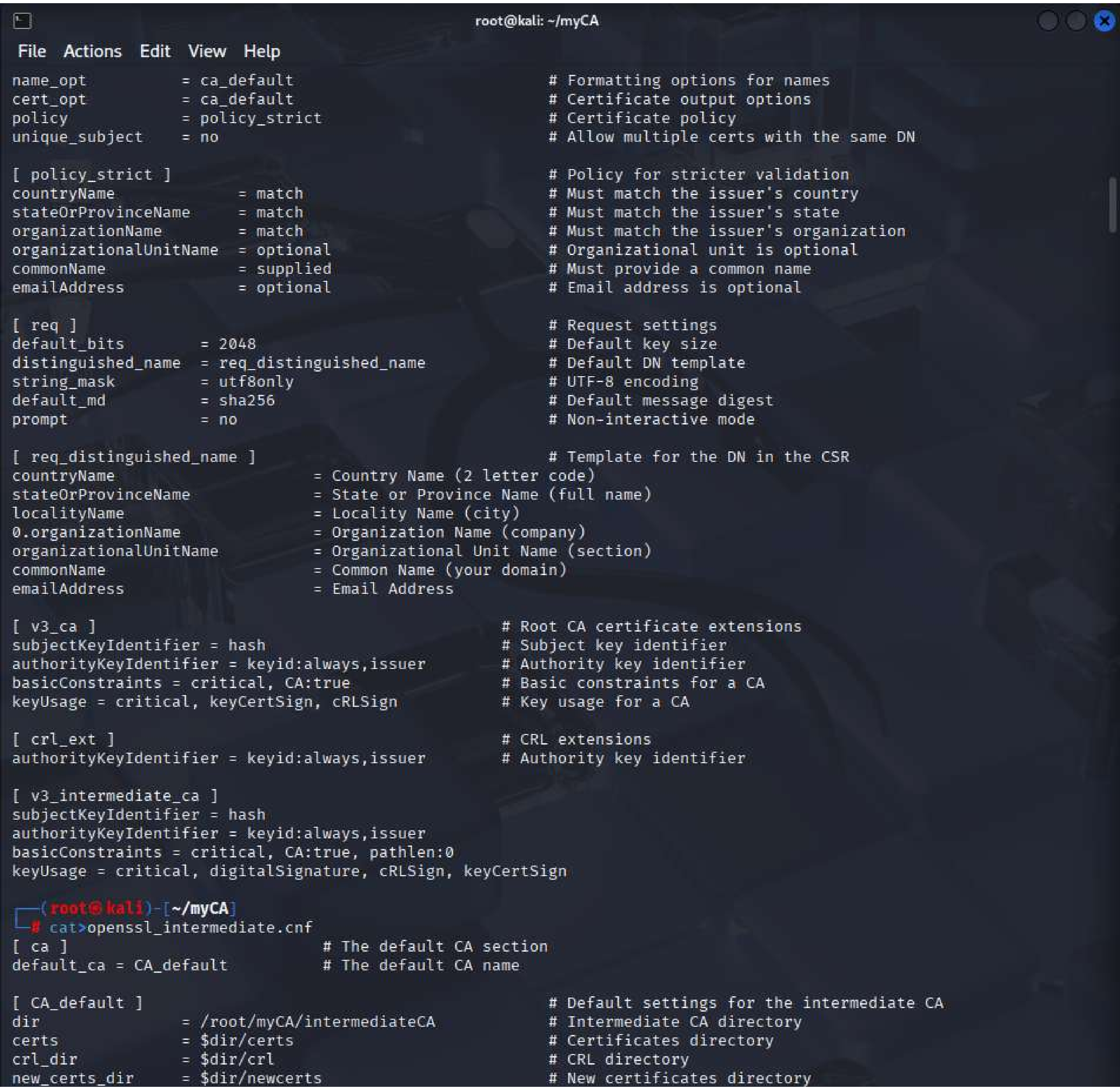


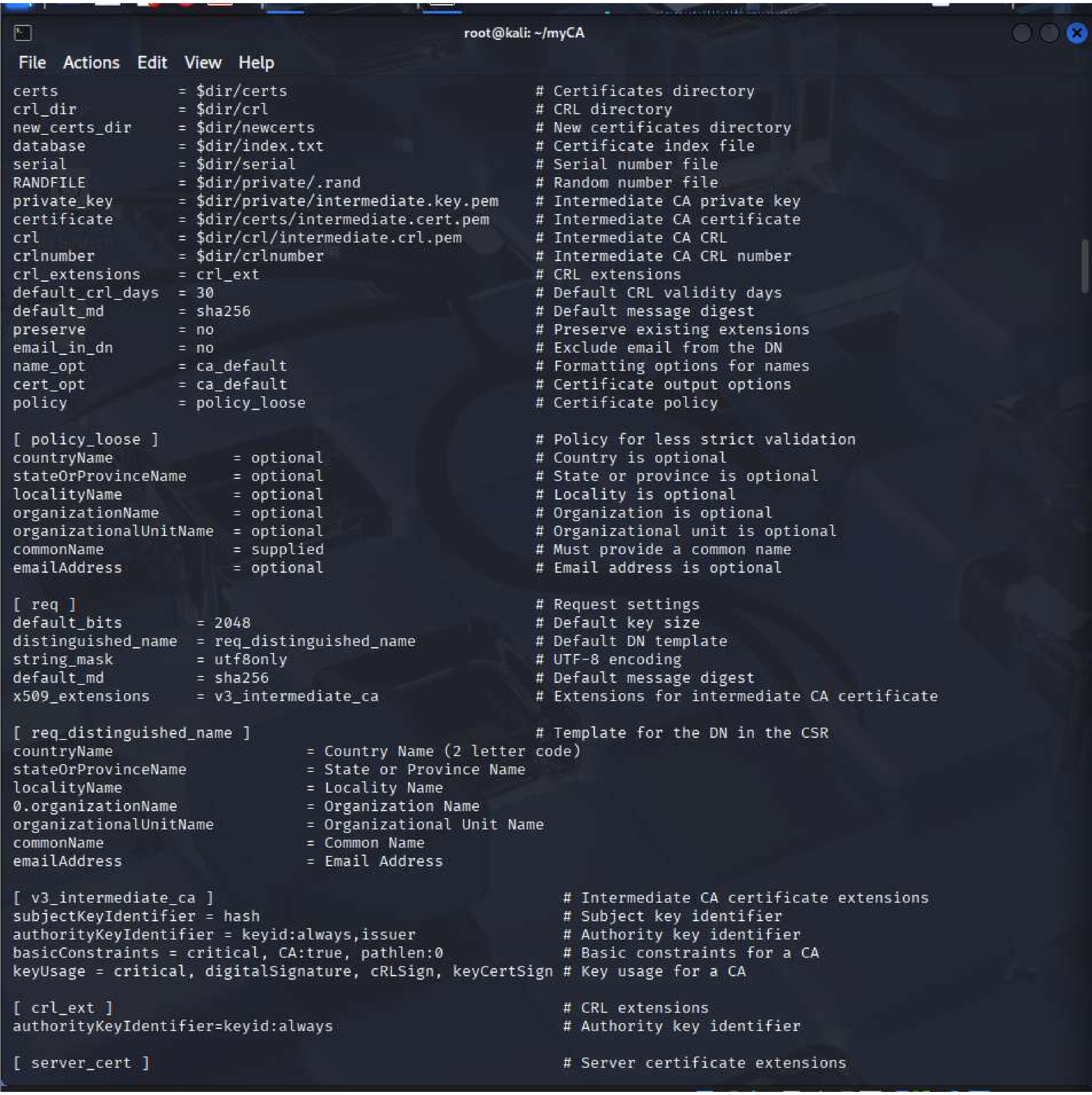
```
┌──(root㉿kali)-[~]
└─# apt install openssl
Upgrading:
  libssl3t64  openssl  openssl-provider-legacy

Summary:
  Upgrading: 3, Installing: 0, Removing: 0, Not Upgrading: 967
  Download size: 4,238 kB
  Space needed: 26.6 kB / 63.7 GB available

Continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 openssl-provider-legacy amd64 3.5.2-1 [307 kB]
Get:3 http://mirror.aktkn.sg/kali kali-rolling/main amd64 openssl amd64 3.5.2-1 [1,493 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libssl3t64 amd64 3.5.2-1 [2,438 kB]
Fetched 4,238 kB in 9s (459 kB/s)
(Reading database ... 412505 files and directories currently installed.)
Preparing to unpack .../openssl-provider-legacy_3.5.2-1_amd64.deb ...
Unpacking openssl-provider-legacy (3.5.2-1) over (3.5.0-1) ...
Setting up openssl-provider-legacy (3.5.2-1) ...
(Reading database ... 412505 files and directories currently installed.)
Preparing to unpack .../libssl3t64_3.5.2-1_amd64.deb ...
Unpacking libssl3t64:amd64 (3.5.2-1) over (3.5.0-1) ...
Setting up libssl3t64:amd64 (3.5.2-1) ...
(Reading database ... 412505 files and directories currently installed.)
Preparing to unpack .../openssl_3.5.2-1_amd64.deb ...
Unpacking openssl (3.5.2-1) over (3.5.0-1) ...
Setting up openssl (3.5.2-1) ...
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...

┌──(root㉿kali)-[~]
└─# apt install openssl
openssl is already the newest version (3.5.2-1).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 967

┌──(root㉿kali)-[~]
└─# mkdir -p ~/myCA/rootCA/{certs,crl,newcerts,private,csr}
mkdir -p ~/myCA/intermediateCA/{certs,crl,newcerts,private,csr}

┌──(root㉿kali)-[~]
└─# echo 1000 > ~/myCA/rootCA/serial
echo 1000 > ~/myCA/intermediateCA/serial

┌──(root㉿kali)-[~]
└─# echo 0100 > ~/myCA/rootCA/crlnumber
echo 0100 > ~/myCA/intermediateCA/crlnumber

┌──(root㉿kali)-[~]
└─# touch ~/myCA/rootCA/index.txt
touch ~/myCA/intermediateCA/index.txt
```



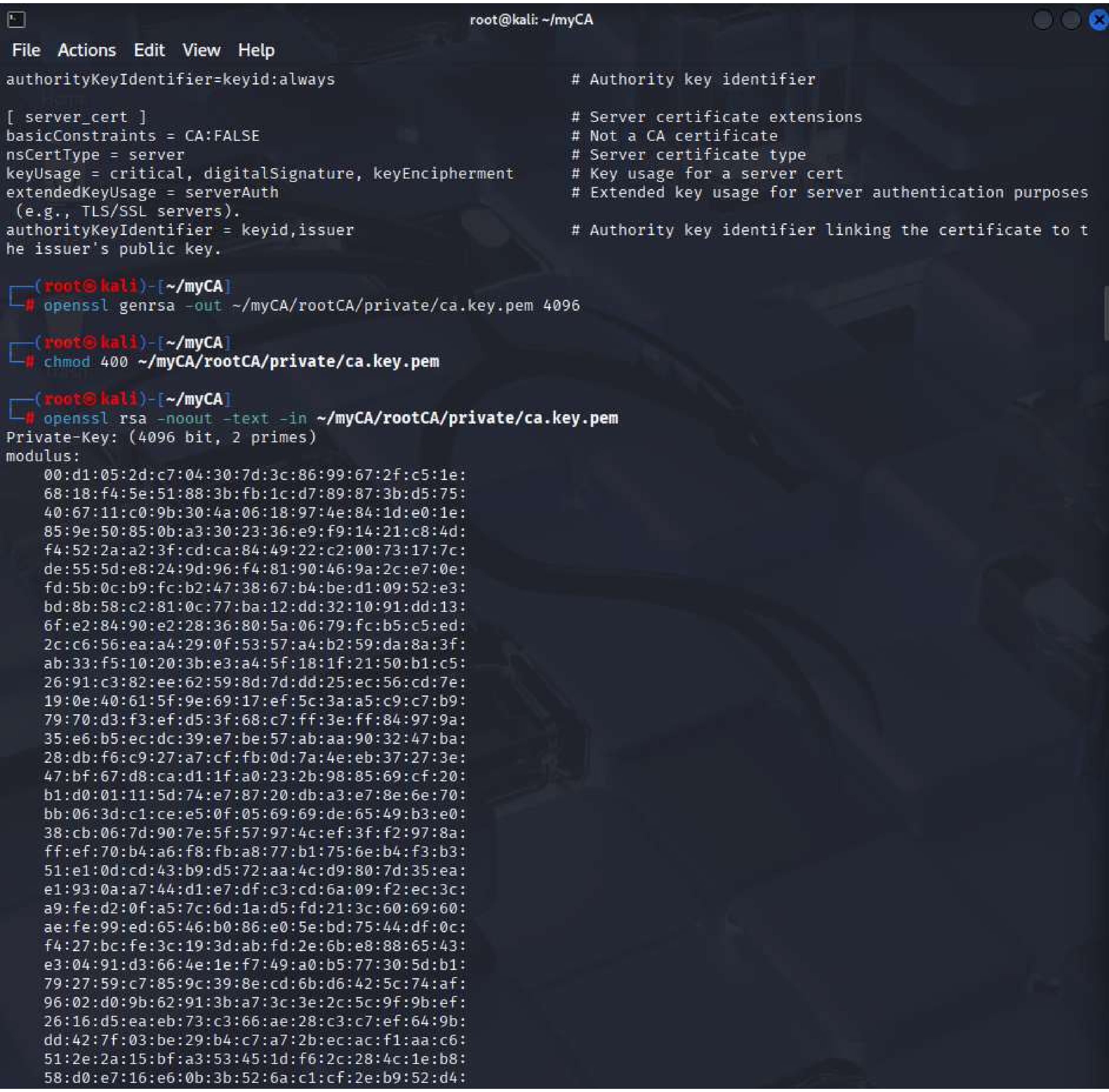
```
touch ~/myCA/intermediateCA/index.txt

┌──(root㉿kali)-[~]
└─# tree ~/myCA
/root/myCA
├── intermediateCA
│   ├── certs
│   ├── crl
│   ├── crlnumber
│   ├── csr
│   ├── index.txt
│   ├── newcerts
│   ├── private
│   └── serial
└── rootCA
    ├── certs
    ├── crl
    ├── crlnumber
    ├── csr
    ├── index.txt
    ├── newcerts
    ├── private
    └── serial

13 directories, 6 files

┌──(root㉿kali)-[~]
└─# cd ~/myCA

┌──(root㉿kali)-[~/myCA]
└─# cat>openssl_root.cnf
[ ca ]                                                     # The default CA section
default_ca = CA_default                                    # The default CA name

[ CA_default ]                                             # Default settings for the CA
dir               = /root/myCA/rootCA                      # CA directory
certs             = $dir/certs                             # Certificates directory
crl_dir           = $dir/crl                               # CRL directory
new_certs_dir     = $dir/newcerts                          # New certificates directory
database          = $dir/index.txt                         # Certificate index file
serial            = $dir/serial                            # Serial number file
RANDFILE          = $dir/private/.rand                     # Random number file
private_key       = $dir/private/ca.key.pem                # Root CA private key
certificate       = $dir/certs/ca.cert.pem                 # Root CA certificate
crl               = $dir/crl/ca.crl.pem                    # Root CA CRL
crlnumber         = $dir/crlnumber                         # Root CA CRL number
crl_extensions    = crl_ext                                # CRL extensions
default_crl_days  = 30                                     # Default CRL validity days
default_md        = sha256                                 # Default message digest
preserve          = no                                     # Preserve existing extensions
email_in_dn       = no                                     # Exclude email from the DN
name_opt          = ca_default                             # Formatting options for names
cert_opt          = ca_default                             # Certificate output options
policy            = policy_strict                          # Certificate policy
```



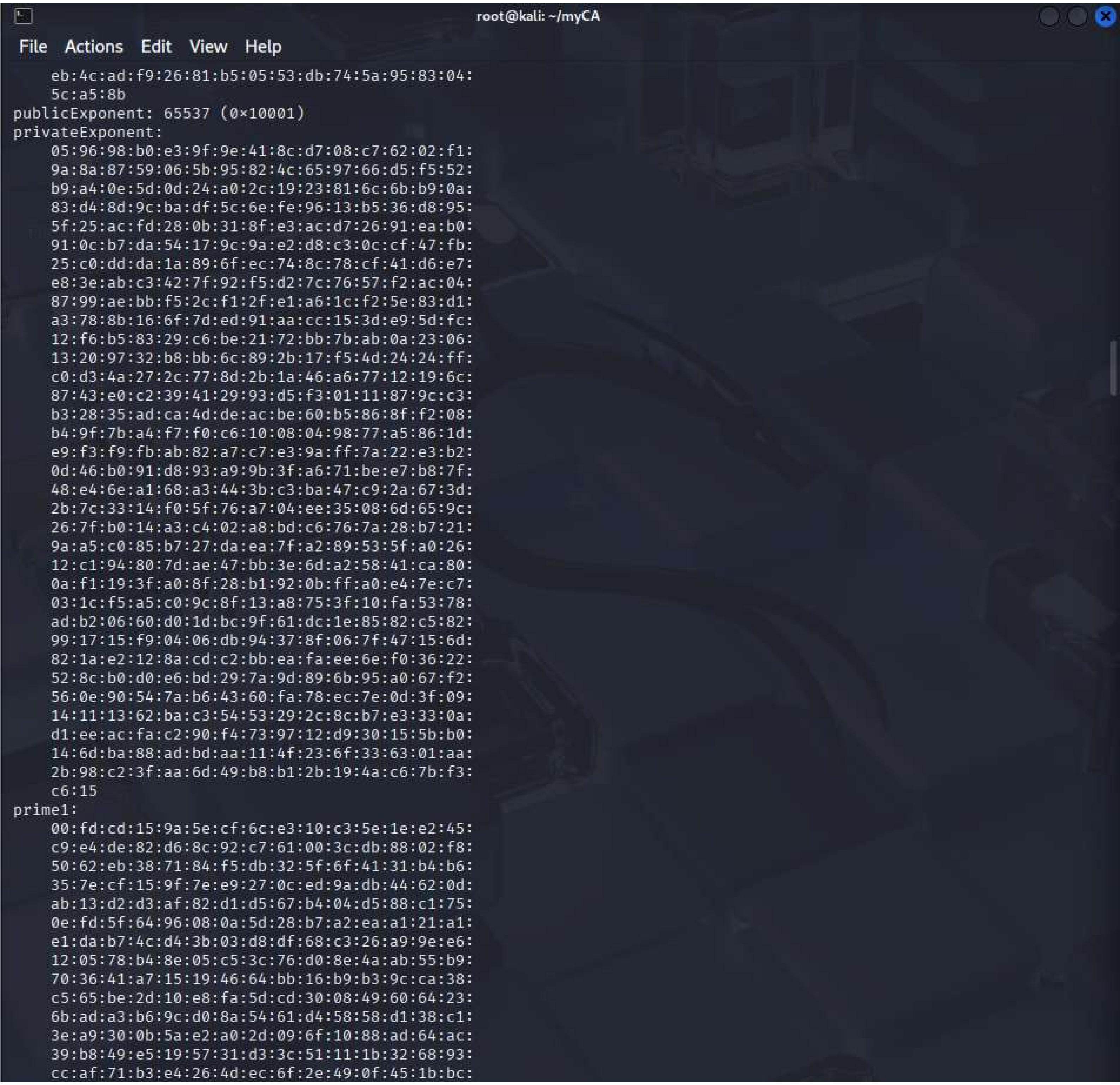
```
name_opt          = ca_default                           # Formatting options for names
cert_opt          = ca_default                           # Certificate output options
policy            = policy_strict                        # Certificate policy
unique_subject    = no                                   # Allow multiple certs with the same DN

[ policy_strict ]                                        # Policy for stricter validation
countryName             = match                          # Must match the issuer's country
stateOrProvinceName     = match                          # Must match the issuer's state
organizationName        = match                          # Must match the issuer's organization
organizationalUnitName  = optional                       # Organizational unit is optional
commonName              = supplied                       # Must provide a common name
emailAddress            = optional                       # Email address is optional

[ req ]                                                  # Request settings
default_bits        = 2048                               # Default key size
distinguished_name  = req_distinguished_name             # Default DN template
string_mask         = utf8only                           # UTF-8 encoding
default_md          = sha256                             # Default message digest
prompt              = no                                 # Non-interactive mode

[ req_distinguished_name ]                               # Template for the DN in the CSR
countryName                     = Country Name (2 letter code)
stateOrProvinceName             = State or Province Name (full name)
localityName                    = Locality Name (city)
0.organizationName              = Organization Name (company)
organizationalUnitName          = Organizational Unit Name (section)
commonName                      = Common Name (your domain)
emailAddress                    = Email Address

[ v3_ca ]                                           # Root CA certificate extensions
subjectKeyIdentifier = hash                         # Subject key identifier
authorityKeyIdentifier = keyid:always,issuer        # Authority key identifier
basicConstraints = critical, CA:true                # Basic constraints for a CA
keyUsage = critical, keyCertSign, cRLSign           # Key usage for a CA

[ crl_ext ]                                         # CRL extensions
authorityKeyIdentifier = keyid:always,issuer        # Authority key identifier

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

┌──(root㉿kali)-[~/myCA]
└─# cat>openssl_intermediate.cnf
[ ca ]                           # The default CA section
default_ca = CA_default          # The default CA name

[ CA_default ]                                           # Default settings for the intermediate CA
dir               = /root/myCA/intermediateCA            # Intermediate CA directory
certs             = $dir/certs                           # Certificates directory
crl_dir           = $dir/crl                             # CRL directory
new_certs_dir     = $dir/newcerts                        # New certificates directory
```



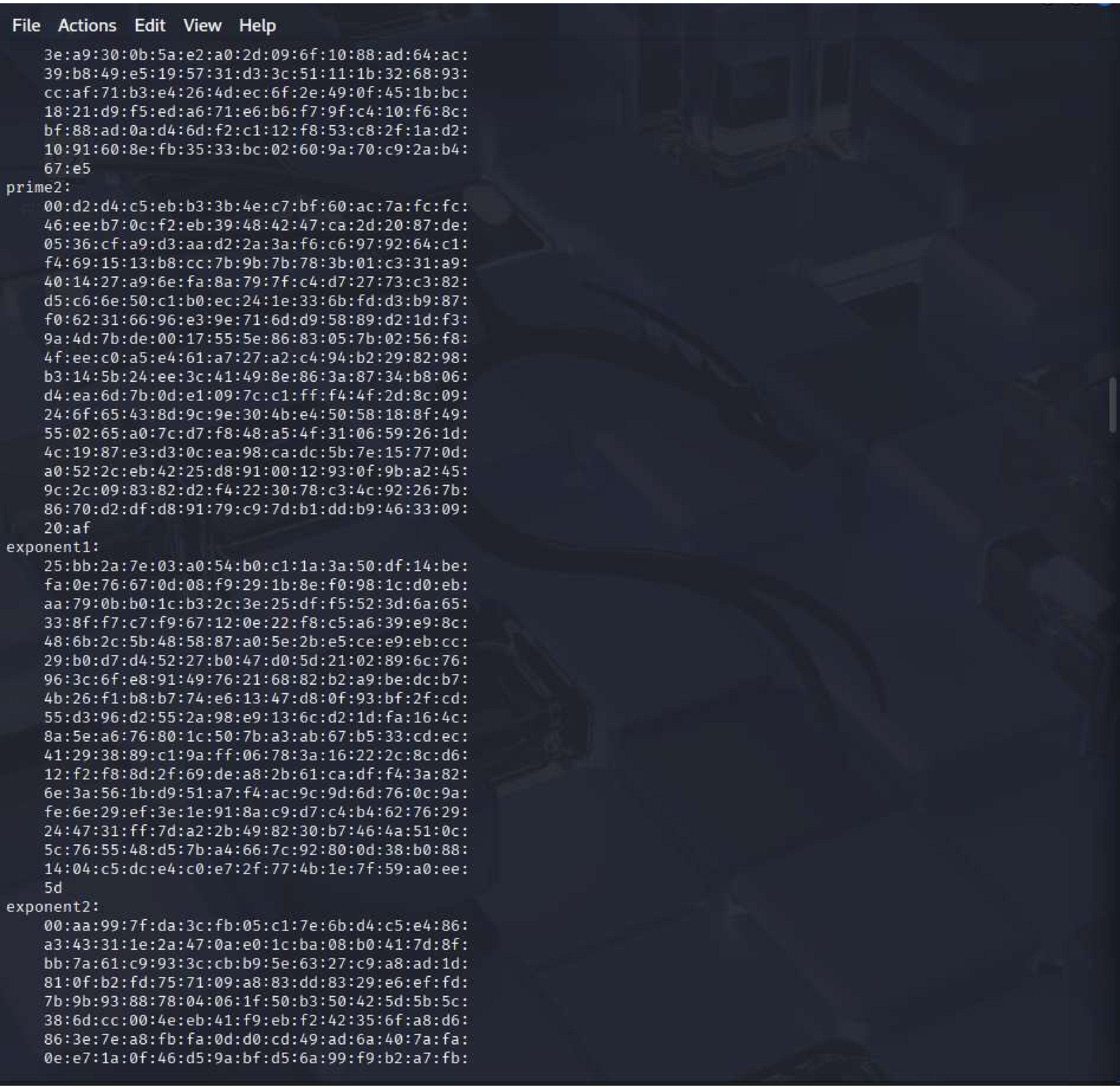
```
certs             = $dir/certs                           # Certificates directory
crl_dir           = $dir/crl                             # CRL directory
new_certs_dir     = $dir/newcerts                        # New certificates directory
database          = $dir/index.txt                       # Certificate index file
serial            = $dir/serial                          # Serial number file
RANDFILE          = $dir/private/.rand                   # Random number file
private_key       = $dir/private/intermediate.key.pem    # Intermediate CA private key
certificate       = $dir/certs/intermediate.cert.pem     # Intermediate CA certificate
crl               = $dir/crl/intermediate.crl.pem        # Intermediate CA CRL
crlnumber         = $dir/crlnumber                       # Intermediate CA CRL number
crl_extensions    = crl_ext                              # CRL extensions
default_crl_days  = 30                                   # Default CRL validity days
default_md        = sha256                               # Default message digest
preserve          = no                                   # Preserve existing extensions
email_in_dn       = no                                   # Exclude email from the DN
name_opt          = ca_default                           # Formatting options for names
cert_opt          = ca_default                           # Certificate output options
policy            = policy_loose                         # Certificate policy

[ policy_loose ]                                         # Policy for less strict validation
countryName             = optional                       # Country is optional
stateOrProvinceName     = optional                       # State or province is optional
localityName            = optional                       # Locality is optional
organizationName        = optional                       # Organization is optional
organizationalUnitName  = optional                       # Organizational unit is optional
commonName              = supplied                       # Must provide a common name
emailAddress            = optional                       # Email address is optional

[ req ]                                                  # Request settings
default_bits        = 2048                               # Default key size
distinguished_name  = req_distinguished_name             # Default DN template
string_mask         = utf8only                           # UTF-8 encoding
default_md          = sha256                             # Default message digest
x509_extensions     = v3_intermediate_ca                 # Extensions for intermediate CA certificate

[ req_distinguished_name ]                               # Template for the DN in the CSR
countryName                     = Country Name (2 letter code)
stateOrProvinceName             = State or Province Name
localityName                    = Locality Name
0.organizationName              = Organization Name
organizationalUnitName          = Organizational Unit Name
commonName                      = Common Name
emailAddress                    = Email Address

[ v3_intermediate_ca ]                                      # Intermediate CA certificate extensions
subjectKeyIdentifier = hash                                 # Subject key identifier
authorityKeyIdentifier = keyid:always,issuer                # Authority key identifier
basicConstraints = critical, CA:true, pathlen:0             # Basic constraints for a CA
keyUsage = critical, digitalSignature, cRLSign, keyCertSign # Key usage for a CA

[ crl_ext ]                                                 # CRL extensions
authorityKeyIdentifier=keyid:always                         # Authority key identifier

[ server_cert ]                                             # Server certificate extensions
```



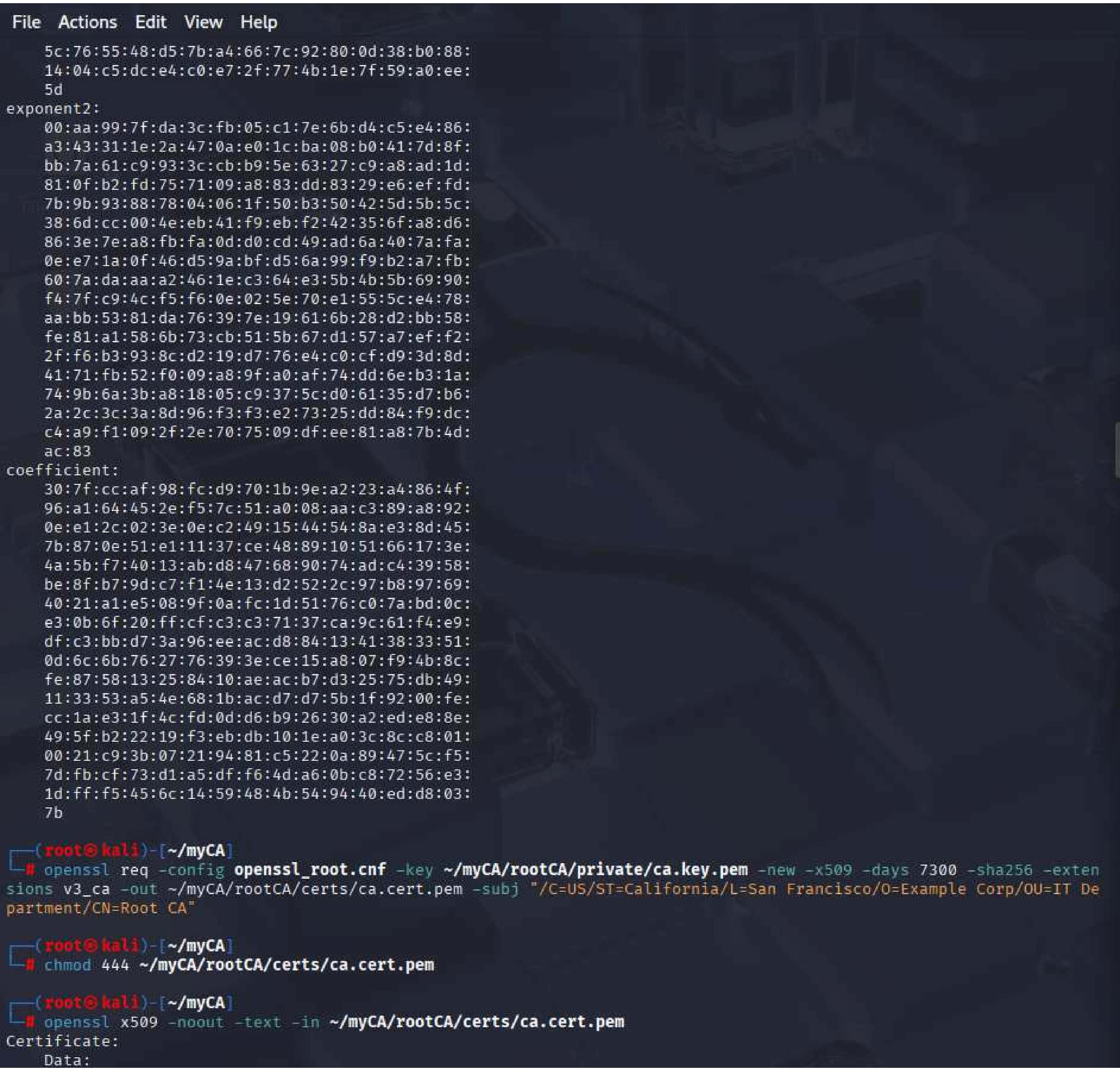
```
authorityKeyIdentifier=keyid:always                          # Authority key identifier

[ server_cert ]                                              # Server certificate extensions
basicConstraints = CA:FALSE                                  # Not a CA certificate
nsCertType = server                                          # Server certificate type
keyUsage = critical, digitalSignature, keyEncipherment       # Key usage for a server cert
extendedKeyUsage = serverAuth                                # Extended key usage for server authentication purposes
 (e.g., TLS/SSL servers).
authorityKeyIdentifier = keyid,issuer                        # Authority key identifier linking the certificate to t
he issuer's public key.

┌──(root㉿kali)-[~/myCA]
└─# openssl genrsa -out ~/myCA/rootCA/private/ca.key.pem 4096

┌──(root㉿kali)-[~/myCA]
└─# chmod 400 ~/myCA/rootCA/private/ca.key.pem

┌──(root㉿kali)-[~/myCA]
└─# openssl rsa -noout -text -in ~/myCA/rootCA/private/ca.key.pem
Private-Key: (4096 bit, 2 primes)
modulus:
    00:d1:05:2d:c7:04:30:7d:3c:86:99:67:2f:c5:1e:
    68:18:f4:5e:51:88:3b:fb:1c:d7:89:87:3b:d5:75:
    40:67:11:c0:9b:30:4a:06:18:97:4e:84:1d:e0:1e:
    85:9e:50:85:0b:a3:30:23:36:e9:f9:14:21:c8:4d:
    f4:52:2a:a2:3f:cd:ca:84:49:22:c2:00:73:17:7c:
    de:55:5d:e8:24:9d:96:f4:81:90:46:9a:2c:e7:0e:
    fd:5b:0c:b9:fc:b2:47:38:67:b4:be:d1:09:52:e3:
    bd:8b:58:c2:81:0c:77:ba:12:dd:32:10:91:dd:13:
    6f:e2:84:90:e2:28:36:80:5a:06:79:fc:b5:c5:ed:
    2c:c6:56:ea:a4:29:0f:53:57:a4:b2:59:da:8a:3f:
    ab:33:f5:10:20:3b:e3:a4:5f:18:1f:21:50:b1:c5:
    26:91:c3:82:ee:62:59:8d:7d:dd:25:ec:56:cd:7e:
    19:0e:40:61:5f:9e:69:17:ef:5c:3a:a5:c9:c7:b9:
    79:70:d3:f3:ef:d5:3f:68:c7:ff:3e:ff:84:97:9a:
    35:e6:b5:ec:dc:39:e7:be:57:ab:aa:90:32:47:ba:
    28:db:f6:c9:27:a7:cf:fb:0d:7a:4e:eb:37:27:3e:
    47:bf:67:d8:ca:d1:1f:a0:23:2b:98:85:69:cf:20:
    b1:d0:01:11:5d:74:e7:87:20:db:a3:e7:8e:6e:70:
    bb:06:3d:c1:ce:e5:0f:05:69:69:de:65:49:b3:e0:
    38:cb:06:7d:90:7e:5f:57:97:4c:ef:3f:f2:97:8a:
    ff:ef:70:b4:a6:f8:fb:a8:77:b1:75:6e:b4:f3:b3:
    51:e1:0d:cd:43:b9:d5:72:aa:4c:d9:80:7d:35:ea:
    e1:93:0a:a7:44:d1:e7:df:c3:cd:6a:09:f2:ec:3c:
    a9:fe:d2:0f:a5:7c:6d:1a:d5:fd:21:3c:60:69:60:
    ae:fe:99:ed:65:46:b0:86:e0:5e:bd:75:44:df:0c:
    f4:27:bc:fe:3c:19:3d:ab:fd:2e:6b:e8:88:65:43:
    e3:04:91:d3:66:4e:1e:f7:49:a0:b5:77:30:5d:b1:
    79:27:59:c7:85:9c:39:8e:cd:6b:d6:42:5c:74:af:
    96:02:d0:9b:62:91:3b:a7:3c:3e:2c:5c:9f:9b:ef:
    26:16:d5:ea:eb:73:c3:66:ae:28:c3:c7:ef:64:9b:
    dd:42:7f:03:be:29:b4:c7:a7:2b:ec:ac:f1:aa:c6:
    51:2e:2a:15:bf:a3:53:45:1d:f6:2c:28:4c:1e:b8:
    58:d0:e7:16:e6:0b:3b:52:6a:c1:cf:2e:b9:52:d4:
```



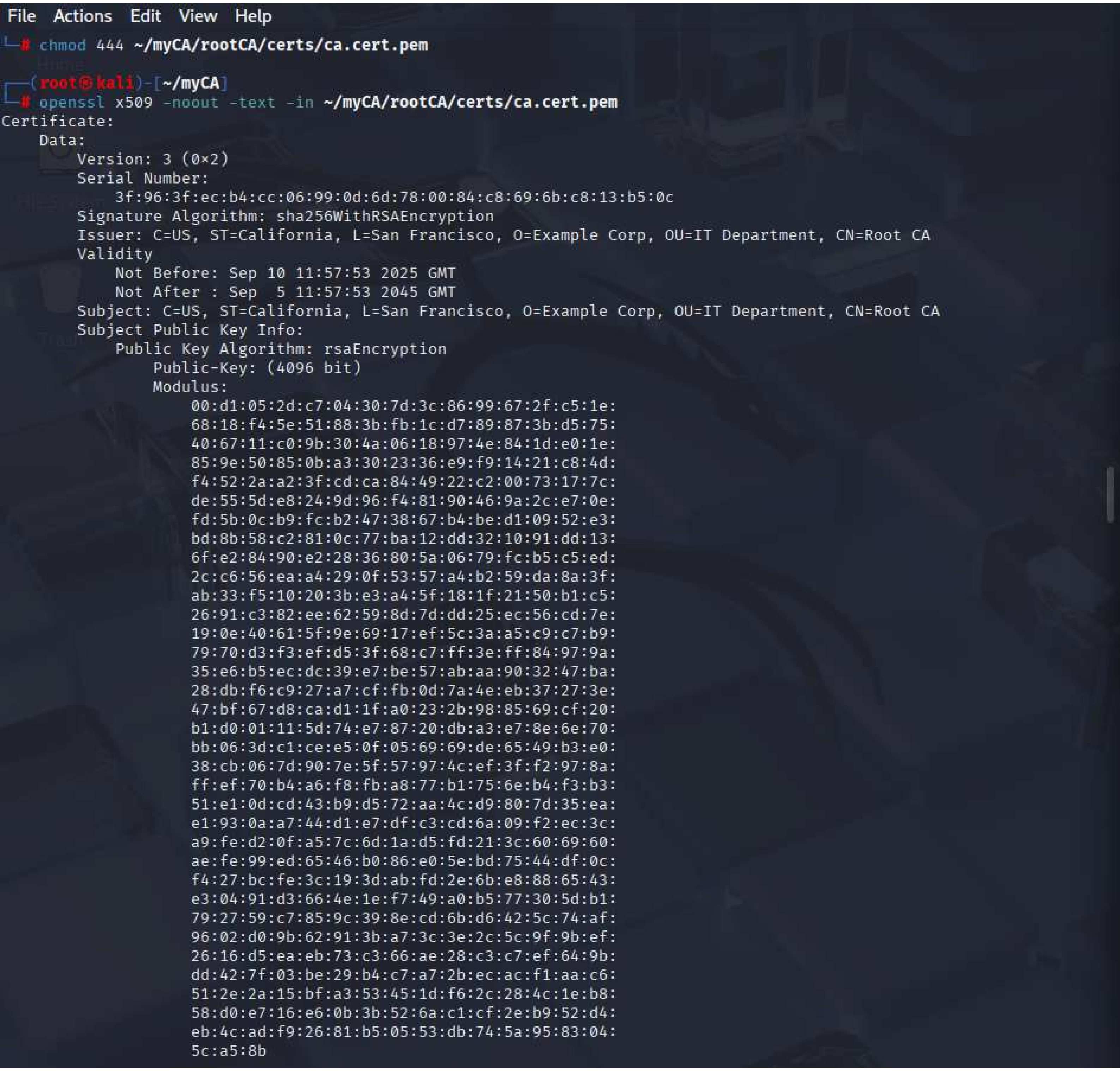
```
    eb:4c:ad:f9:26:81:b5:05:53:db:74:5a:95:83:04:
    5c:a5:8b
publicExponent: 65537 (0×10001)
privateExponent:
    05:96:98:b0:e3:9f:9e:41:8c:d7:08:c7:62:02:f1:
    9a:8a:87:59:06:5b:95:82:4c:65:97:66:d5:f5:52:
    b9:a4:0e:5d:0d:24:a0:2c:19:23:81:6c:6b:b9:0a:
    83:d4:8d:9c:ba:df:5c:6e:fe:96:13:b5:36:d8:95:
    5f:25:ac:fd:28:0b:31:8f:e3:ac:d7:26:91:ea:b0:
    91:0c:b7:da:54:17:9c:9a:e2:d8:c3:0c:cf:47:fb:
    25:c0:dd:da:1a:89:6f:ec:74:8c:78:cf:41:d6:e7:
    e8:3e:ab:c3:42:7f:92:f5:d2:7c:76:57:f2:ac:04:
    87:99:ae:bb:f5:2c:f1:2f:e1:a6:1c:f2:5e:83:d1:
    a3:78:8b:16:6f:7d:ed:91:aa:cc:15:3d:e9:5d:fc:
    12:f6:b5:83:29:c6:be:21:72:bb:7b:ab:0a:23:06:
    13:20:97:32:b8:bb:6c:89:2b:17:f5:4d:24:24:ff:
    c0:d3:4a:27:2c:77:8d:2b:1a:46:a6:77:12:19:6c:
    87:43:e0:c2:39:41:29:93:d5:f3:01:11:87:9c:c3:
    b3:28:35:ad:ca:4d:de:ac:be:60:b5:86:8f:f2:08:
    b4:9f:7b:a4:f7:f0:c6:10:08:04:98:77:a5:86:1d:
    e9:f3:f9:fb:ab:82:a7:c7:e3:9a:ff:7a:22:e3:b2:
    0d:46:b0:91:d8:93:a9:9b:3f:a6:71:be:e7:b8:7f:
    48:e4:6e:a1:68:a3:44:3b:c3:ba:47:c9:2a:67:3d:
    2b:7c:33:14:f0:5f:76:a7:04:ee:35:08:6d:65:9c:
    26:7f:b0:14:a3:c4:02:a8:bd:c6:76:7a:28:b7:21:
    9a:a5:c0:85:b7:27:da:ea:7f:a2:89:53:5f:a0:26:
    12:c1:94:80:7d:ae:47:bb:3e:6d:a2:58:41:ca:80:
    0a:f1:19:3f:a0:8f:28:b1:92:0b:ff:a0:e4:7e:c7:
    03:1c:f5:a5:c0:9c:8f:13:a8:75:3f:10:fa:53:78:
    ad:b2:06:60:d0:1d:bc:9f:61:dc:1e:85:82:c5:82:
    99:17:15:f9:04:06:db:94:37:8f:06:7f:47:15:6d:
    82:1a:e2:12:8a:cd:c2:bb:ea:fa:ee:6e:f0:36:22:
    52:8c:b0:d0:e6:bd:29:7a:9d:89:6b:95:a0:67:f2:
    56:0e:90:54:7a:b6:43:60:fa:78:ec:7e:0d:3f:09:
    14:11:13:62:ba:c3:54:53:29:2c:8c:b7:e3:33:0a:
    d1:ee:ac:fa:c2:90:f4:73:97:12:d9:30:15:5b:b0:
    14:6d:ba:88:ad:bd:aa:11:4f:23:6f:33:63:01:aa:
    2b:98:c2:3f:aa:6d:49:b8:b1:2b:19:4a:c6:7b:f3:
    c6:15
prime1:
    00:fd:cd:15:9a:5e:cf:6c:e3:10:c3:5e:1e:e2:45:
    c9:e4:de:82:d6:8c:92:c7:61:00:3c:db:88:02:f8:
    50:62:eb:38:71:84:f5:db:32:5f:6f:41:31:b4:b6:
    35:7e:cf:15:9f:7e:e9:27:0c:ed:9a:db:44:62:0d:
    ab:13:d2:d3:af:82:d1:d5:67:b4:04:d5:88:c1:75:
    0e:fd:5f:64:96:08:0a:5d:28:b7:a2:ea:a1:21:a1:
    e1:da:b7:4c:d4:3b:03:d8:df:68:c3:26:a9:9e:e6:
    12:05:78:b4:8e:05:c5:3c:76:d0:8e:4a:ab:55:b9:
    70:36:41:a7:15:19:46:64:bb:16:b9:b3:9c:ca:38:
    c5:65:be:2d:10:e8:fa:5d:cd:30:08:49:60:64:23:
    6b:ad:a3:b6:9c:d0:8a:54:61:d4:58:58:d1:38:c1:
    3e:a9:30:0b:5a:e2:a0:2d:09:6f:10:88:ad:64:ac:
    39:b8:49:e5:19:57:31:d3:3c:51:11:1b:32:68:93:
    cc:af:71:b3:e4:26:4d:ec:6f:2e:49:0f:45:1b:bc:
```



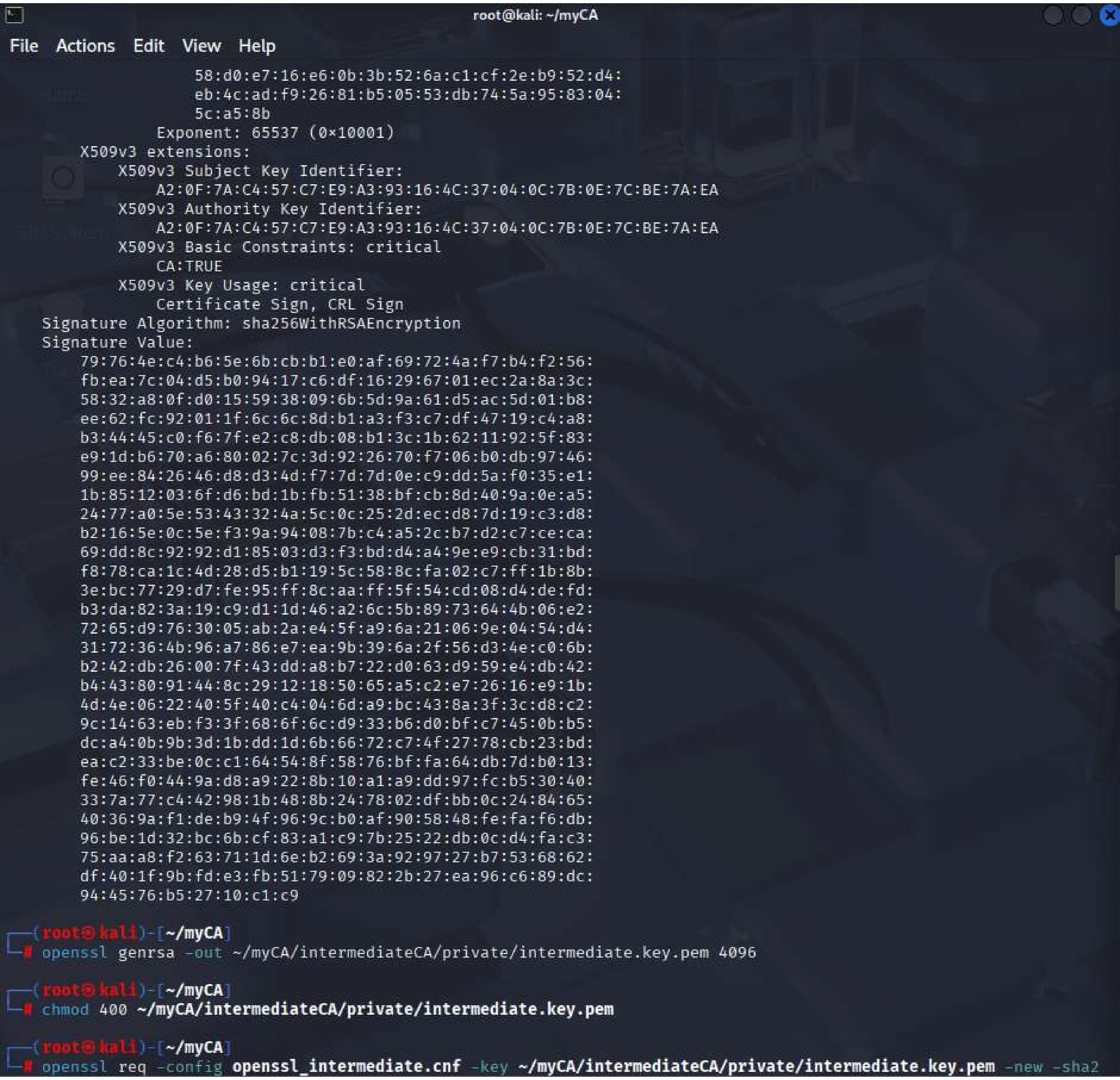
```
    3e:a9:30:0b:5a:e2:a0:2d:09:6f:10:88:ad:64:ac:
    39:b8:49:e5:19:57:31:d3:3c:51:11:1b:32:68:93:
    cc:af:71:b3:e4:26:4d:ec:6f:2e:49:0f:45:1b:bc:
    18:21:d9:f5:ed:a6:71:e6:b6:f7:9f:c4:10:f6:8c:
    bf:88:ad:0a:d4:6d:f2:c1:12:f8:53:c8:2f:1a:d2:
    10:91:60:8e:fb:35:33:bc:02:60:9a:70:c9:2a:b4:
    67:e5
prime2:
    00:d2:d4:c5:eb:b3:3b:4e:c7:bf:60:ac:7a:fc:fc:
    46:ee:b7:0c:f2:eb:39:48:42:47:ca:2d:20:87:de:
    05:36:cf:a9:d3:aa:d2:2a:3a:f6:c6:97:92:64:c1:
    f4:69:15:13:b8:cc:7b:9b:7b:78:3b:01:c3:31:a9:
    40:14:27:a9:6e:fa:8a:79:7f:c4:d7:27:73:c3:82:
    d5:c6:6e:50:c1:b0:ec:24:1e:33:6b:fd:d3:b9:87:
    f0:62:31:66:96:e3:9e:71:6d:d9:58:89:d2:1d:f3:
    9a:4d:7b:de:00:17:55:5e:86:83:05:7b:02:56:f8:
    4f:ee:c0:a5:e4:61:a7:27:a2:c4:94:b2:29:82:98:
    b3:14:5b:24:ee:3c:41:49:8e:86:3a:87:34:b8:06:
    d4:ea:6d:7b:0d:e1:09:7c:c1:ff:f4:4f:2d:8c:09:
    24:6f:65:43:8d:9c:9e:30:4b:e4:50:58:18:8f:49:
    55:02:65:a0:7c:d7:f8:48:a5:4f:31:06:59:26:1d:
    4c:19:87:e3:d3:0c:ea:98:ca:dc:5b:7e:15:77:0d:
    a0:52:2c:eb:42:25:d8:91:00:12:93:0f:9b:a2:45:
    9c:2c:09:83:82:d2:f4:22:30:78:c3:4c:92:26:7b:
    86:70:d2:df:d8:91:79:c9:7d:b1:dd:b9:46:33:09:
    20:af
exponent1:
    25:bb:2a:7e:03:a0:54:b0:c1:1a:3a:50:df:14:be:
    fa:0e:76:67:0d:08:f9:29:1b:8e:f0:98:1c:d0:eb:
    aa:79:0b:b0:1c:b3:2c:3e:25:df:f5:52:3d:6a:65:
    33:8f:f7:c7:f9:67:12:0e:22:f8:c5:a6:39:e9:8c:
    48:6b:2c:5b:48:58:87:a0:5e:2b:e5:ce:e9:eb:cc:
    29:b0:d7:d4:52:27:b0:47:d0:5d:21:02:89:6c:76:
    96:3c:6f:e8:91:49:76:21:68:82:b2:a9:be:dc:b7:
    4b:26:f1:b8:b7:74:e6:13:47:d8:0f:93:bf:2f:cd:
    55:d3:96:d2:55:2a:98:e9:13:6c:d2:1d:fa:16:4c:
    8a:5e:a6:76:80:1c:50:7b:a3:ab:67:b5:33:cd:ec:
    41:29:38:89:c1:9a:ff:06:78:3a:16:22:2c:8c:d6:
    12:f2:f8:8d:2f:69:de:a8:2b:61:ca:df:f4:3a:82:
    6e:3a:56:1b:d9:51:a7:f4:ac:9c:9d:6d:76:0c:9a:
    fe:6e:29:ef:3e:1e:91:8a:c9:d7:c4:b4:62:76:29:
    24:47:31:ff:7d:a2:2b:49:82:30:b7:46:4a:51:0c:
    5c:76:55:48:d5:7b:a4:66:7c:92:80:0d:38:b0:88:
    14:04:c5:dc:e4:c0:e7:2f:77:4b:1e:7f:59:a0:ee:
    5d
exponent2:
    00:aa:99:7f:da:3c:fb:05:c1:7e:6b:d4:c5:e4:86:
    a3:43:31:1e:2a:47:0a:e0:1c:ba:08:b0:41:7d:8f:
    bb:7a:61:c9:93:3c:cb:b9:5e:63:27:c9:a8:ad:1d:
    81:0f:b2:fd:75:71:09:a8:83:dd:83:29:e6:ef:fd:
    7b:9b:93:88:78:04:06:1f:50:b3:50:42:5d:5b:5c:
    38:6d:cc:00:4e:eb:41:f9:eb:f2:42:35:6f:a8:d6:
    86:3e:7e:a8:fb:fa:0d:d0:cd:49:ad:6a:40:7a:fa:
    0e:e7:1a:0f:46:d5:9a:bf:d5:6a:99:f9:b2:a7:fb:
```



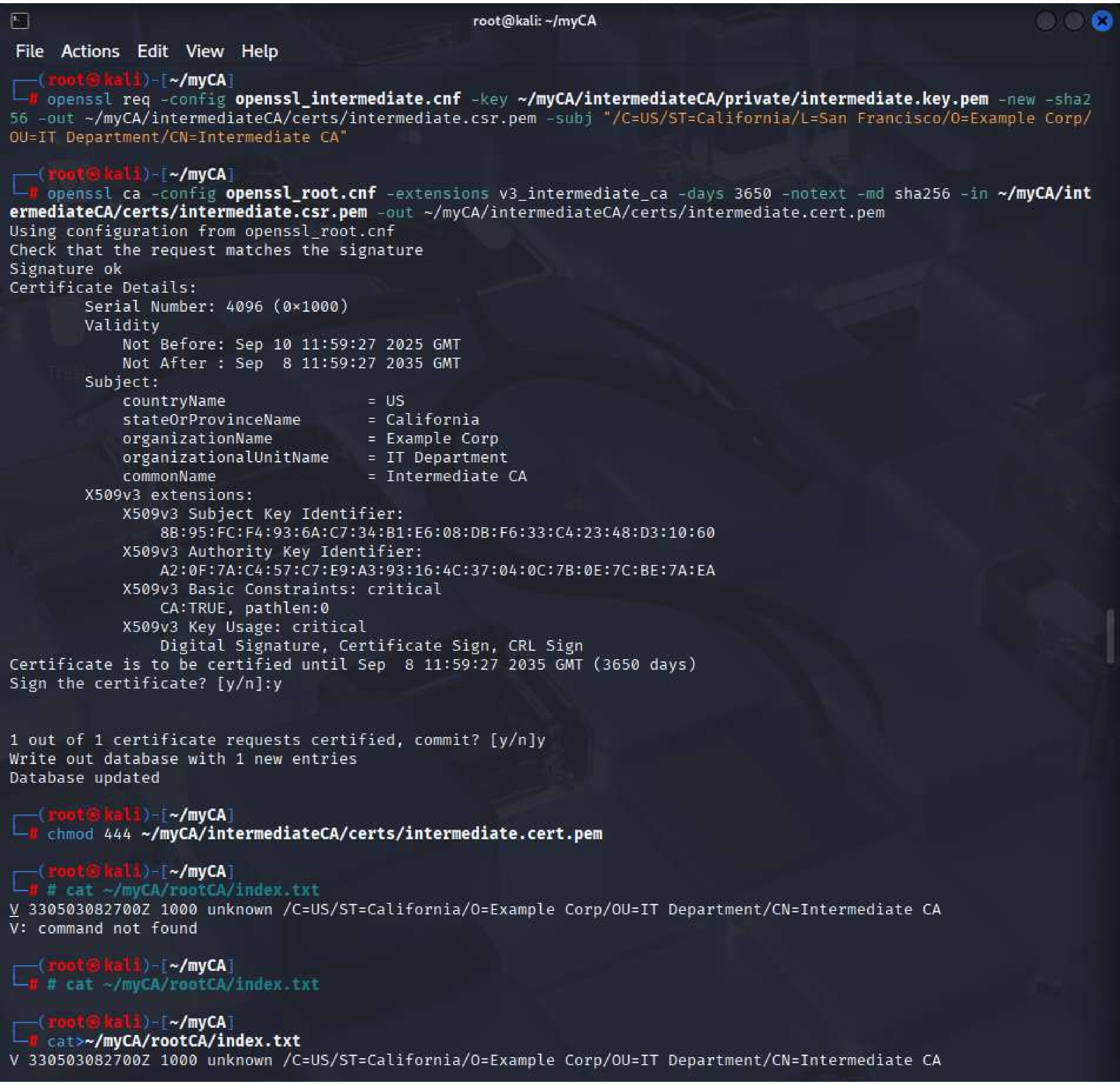
```
    5c:76:55:48:d5:7b:a4:66:7c:92:80:0d:38:b0:88:
    14:04:c5:dc:e4:c0:e7:2f:77:4b:1e:7f:59:a0:ee:
    5d
exponent2:
    00:aa:99:7f:da:3c:fb:05:c1:7e:6b:d4:c5:e4:86:
    a3:43:31:1e:2a:47:0a:e0:1c:ba:08:b0:41:7d:8f:
    bb:7a:61:c9:93:3c:cb:b9:5e:63:27:c9:a8:ad:1d:
    81:0f:b2:fd:75:71:09:a8:83:dd:83:29:e6:ef:fd:
    7b:9b:93:88:78:04:06:1f:50:b3:50:42:5d:5b:5c:
    38:6d:cc:00:4e:eb:41:f9:eb:f2:42:35:6f:a8:d6:
    86:3e:7e:a8:fb:fa:0d:d0:cd:49:ad:6a:40:7a:fa:
    0e:e7:1a:0f:46:d5:9a:bf:d5:6a:99:f9:b2:a7:fb:
    60:7a:da:aa:a2:46:1e:c3:64:e3:5b:4b:5b:69:90:
    f4:7f:c9:4c:f5:f6:0e:02:5e:70:e1:55:5c:e4:78:
    aa:bb:53:81:da:76:39:7e:19:61:6b:28:d2:bb:58:
    fe:81:a1:58:6b:73:cb:51:5b:67:d1:57:a7:ef:f2:
    2f:f6:b3:93:8c:d2:19:d7:76:e4:c0:cf:d9:3d:8d:
    41:71:fb:52:f0:09:a8:9f:a0:af:74:dd:6e:b3:1a:
    74:9b:6a:3b:a8:18:05:c9:37:5c:d0:61:35:d7:b6:
    2a:2c:3c:3a:8d:96:f3:f3:e2:73:25:dd:84:f9:dc:
    c4:a9:f1:09:2f:2e:70:75:09:df:ee:81:a8:7b:4d:
    ac:83
coefficient:
    30:7f:cc:af:98:fc:d9:70:1b:9e:a2:23:a4:86:4f:
    96:a1:64:45:2e:f5:7c:51:a0:08:aa:c3:89:a8:92:
    0e:e1:2c:02:3e:0e:c2:49:15:44:54:8a:e3:8d:45:
    7b:87:0e:51:e1:11:37:ce:48:89:10:51:66:17:3e:
    4a:5b:f7:40:13:ab:d8:47:68:90:74:ad:c4:39:58:
    be:8f:b7:9d:c7:f1:4e:13:d2:52:2c:97:b8:97:69:
    40:21:a1:e5:08:9f:0a:fc:1d:51:76:c0:7a:bd:0c:
    e3:0b:6f:20:ff:cf:c3:c3:71:37:ca:9c:61:f4:e9:
    df:c3:bb:d7:3a:96:ee:ac:d8:84:13:41:38:33:51:
    0d:6c:6b:76:27:76:39:3e:ce:15:a8:07:f9:4b:8c:
    fe:87:58:13:25:84:10:ae:ac:b7:d3:25:75:db:49:
    11:33:53:a5:4e:68:1b:ac:d7:d7:5b:1f:92:00:fe:
    cc:1a:e3:1f:4c:fd:0d:d6:b9:26:30:a2:ed:e8:8e:
    49:5f:b2:22:19:f3:eb:db:10:1e:a0:3c:8c:c8:01:
    00:21:c9:3b:07:21:94:81:c5:22:0a:89:47:5c:f5:
    7d:fb:cf:73:d1:a5:df:f6:4d:a6:0b:c8:72:56:e3:
    1d:ff:f5:45:6c:14:59:48:4b:54:94:40:ed:d8:03:
    7b

┌──(root㉿kali)-[~/myCA]
└─# openssl req -config openssl_root.cnf -key ~/myCA/rootCA/private/ca.key.pem -new -x509 -days 7300 -sha256 -exten
sions v3_ca -out ~/myCA/rootCA/certs/ca.cert.pem -subj "/C=US/ST=California/L=San Francisco/O=Example Corp/OU=IT De
partment/CN=Root CA"

┌──(root㉿kali)-[~/myCA]
└─# chmod 444 ~/myCA/rootCA/certs/ca.cert.pem

┌──(root㉿kali)-[~/myCA]
└─# openssl x509 -noout -text -in ~/myCA/rootCA/certs/ca.cert.pem
Certificate:
    Data:
```



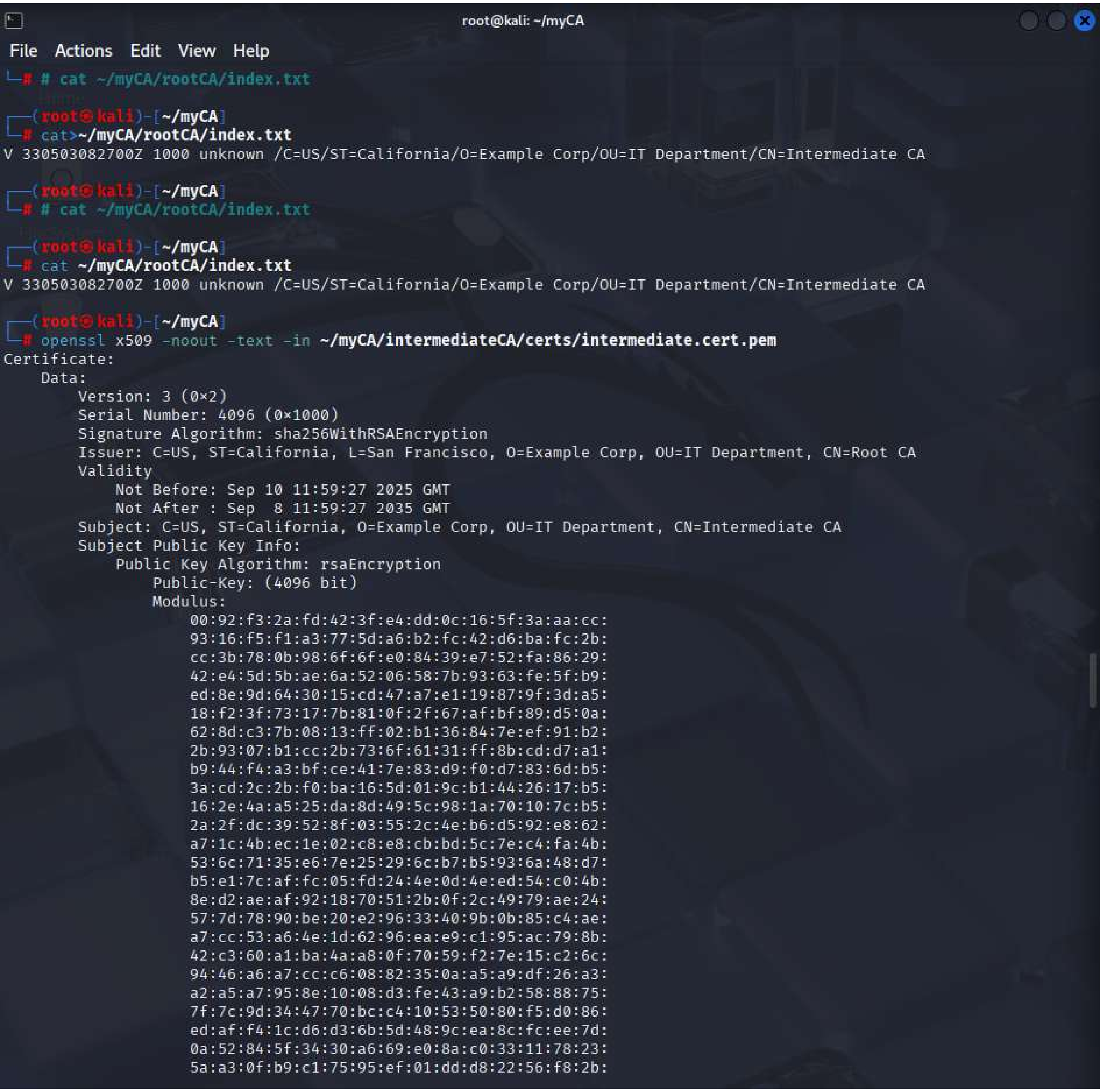
```
└─# chmod 444 ~/myCA/rootCA/certs/ca.cert.pem

┌──(root㉿kali)-[~/myCA]
└─# openssl x509 -noout -text -in ~/myCA/rootCA/certs/ca.cert.pem
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            3f:96:3f:ec:b4:cc:06:99:0d:6d:78:00:84:c8:69:6b:c8:13:b5:0c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, L=San Francisco, O=Example Corp, OU=IT Department, CN=Root CA
        Validity
            Not Before: Sep 10 11:57:53 2025 GMT
            Not After : Sep  5 11:57:53 2045 GMT
        Subject: C=US, ST=California, L=San Francisco, O=Example Corp, OU=IT Department, CN=Root CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:d1:05:2d:c7:04:30:7d:3c:86:99:67:2f:c5:1e:
                    68:18:f4:5e:51:88:3b:fb:1c:d7:89:87:3b:d5:75:
                    40:67:11:c0:9b:30:4a:06:18:97:4e:84:1d:e0:1e:
                    85:9e:50:85:0b:a3:30:23:36:e9:f9:14:21:c8:4d:
                    f4:52:2a:a2:3f:cd:ca:84:49:22:c2:00:73:17:7c:
                    de:55:5d:e8:24:9d:96:f4:81:90:46:9a:2c:e7:0e:
                    fd:5b:0c:b9:fc:b2:47:38:67:b4:be:d1:09:52:e3:
                    bd:8b:58:c2:81:0c:77:ba:12:dd:32:10:91:dd:13:
                    6f:e2:84:90:e2:28:36:80:5a:06:79:fc:b5:c5:ed:
                    2c:c6:56:ea:a4:29:0f:53:57:a4:b2:59:da:8a:3f:
                    ab:33:f5:10:20:3b:e3:a4:5f:18:1f:21:50:b1:c5:
                    26:91:c3:82:ee:62:59:8d:7d:dd:25:ec:56:cd:7e:
                    19:0e:40:61:5f:9e:69:17:ef:5c:3a:a5:c9:c7:b9:
                    79:70:d3:f3:ef:d5:3f:68:c7:ff:3e:ff:84:97:9a:
                    35:e6:b5:ec:dc:39:e7:be:57:ab:aa:90:32:47:ba:
                    28:db:f6:c9:27:a7:cf:fb:0d:7a:4e:eb:37:27:3e:
                    47:bf:67:d8:ca:d1:1f:a0:23:2b:98:85:69:cf:20:
                    b1:d0:01:11:5d:74:e7:87:20:db:a3:e7:8e:6e:70:
                    bb:06:3d:c1:ce:e5:0f:05:69:69:de:65:49:b3:e0:
                    38:cb:06:7d:90:7e:5f:57:97:4c:ef:3f:f2:97:8a:
                    ff:ef:70:b4:a6:f8:fb:a8:77:b1:75:6e:b4:f3:b3:
                    51:e1:0d:cd:43:b9:d5:72:aa:4c:d9:80:7d:35:ea:
                    e1:93:0a:a7:44:d1:e7:df:c3:cd:6a:09:f2:ec:3c:
                    a9:fe:d2:0f:a5:7c:6d:1a:d5:fd:21:3c:60:69:60:
                    ae:fe:99:ed:65:46:b0:86:e0:5e:bd:75:44:df:0c:
                    f4:27:bc:fe:3c:19:3d:ab:fd:2e:6b:e8:88:65:43:
                    e3:04:91:d3:66:4e:1e:f7:49:a0:b5:77:30:5d:b1:
                    79:27:59:c7:85:9c:39:8e:cd:6b:d6:42:5c:74:af:
                    96:02:d0:9b:62:91:3b:a7:3c:3e:2c:5c:9f:9b:ef:
                    26:16:d5:ea:eb:73:c3:66:ae:28:c3:c7:ef:64:9b:
                    dd:42:7f:03:be:29:b4:c7:a7:2b:ec:ac:f1:aa:c6:
                    51:2e:2a:15:bf:a3:53:45:1d:f6:2c:28:4c:1e:b8:
                    58:d0:e7:16:e6:0b:3b:52:6a:c1:cf:2e:b9:52:d4:
                    eb:4c:ad:f9:26:81:b5:05:53:db:74:5a:95:83:04:
                    5c:a5:8b
```



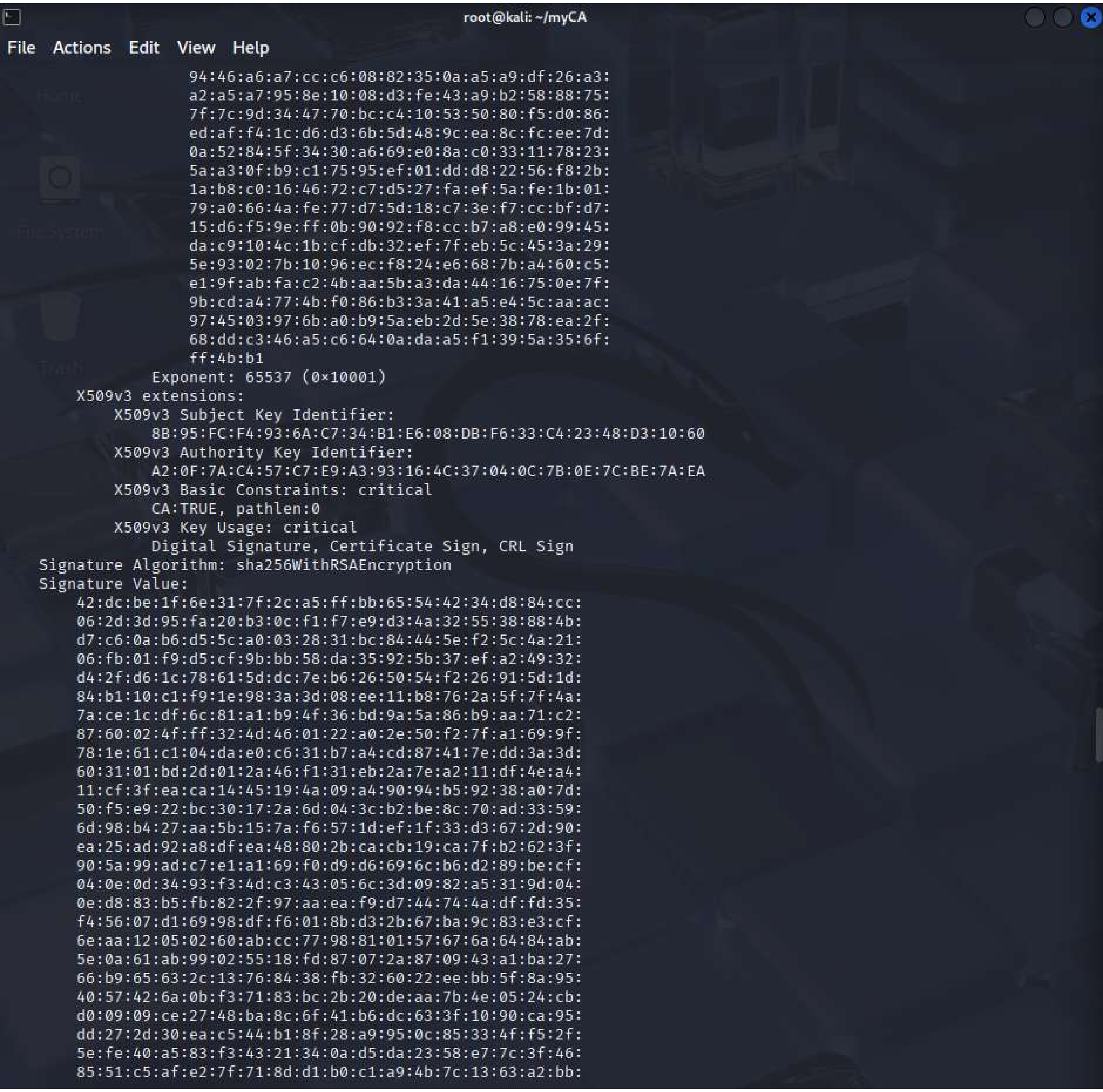
```
                58:d0:e7:16:e6:0b:3b:52:6a:c1:cf:2e:b9:52:d4:
                eb:4c:ad:f9:26:81:b5:05:53:db:74:5a:95:83:04:
                5c:a5:8b
            Exponent: 65537 (0×10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            A2:0F:7A:C4:57:C7:E9:A3:93:16:4C:37:04:0C:7B:0E:7C:BE:7A:EA
        X509v3 Authority Key Identifier:
            A2:0F:7A:C4:57:C7:E9:A3:93:16:4C:37:04:0C:7B:0E:7C:BE:7A:EA
        X509v3 Basic Constraints: critical
            CA:TRUE
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
    79:76:4e:c4:b6:5e:6b:cb:b1:e0:af:69:72:4a:f7:b4:f2:56:
    fb:ea:7c:04:d5:b0:94:17:c6:df:16:29:67:01:ec:2a:8a:3c:
    58:32:a8:0f:d0:15:59:38:09:6b:5d:9a:61:d5:ac:5d:01:b8:
    ee:62:fc:92:01:1f:6c:6c:8d:b1:a3:f3:c7:df:47:19:c4:a8:
    b3:44:45:c0:f6:7f:e2:c8:db:08:b1:3c:1b:62:11:92:5f:83:
    e9:1d:b6:70:a6:80:02:7c:3d:92:26:70:f7:06:b0:db:97:46:
    99:ee:84:26:46:d8:d3:4d:f7:7d:7d:0e:c9:dd:5a:f0:35:e1:
    1b:85:12:03:6f:d6:bd:1b:fb:51:38:bf:cb:8d:40:9a:0e:a5:
    24:77:a0:5e:53:43:32:4a:5c:0c:25:2d:ec:d8:7d:19:c3:d8:
    b2:16:5e:0c:5e:f3:9a:94:08:7b:c4:a5:2c:b7:d2:c7:ce:ca:
    69:dd:8c:92:92:d1:85:03:d3:f3:bd:d4:a4:9e:e9:cb:31:bd:
    f8:78:ca:1c:4d:28:d5:b1:19:5c:58:8c:fa:02:c7:ff:1b:8b:
    3e:bc:77:29:d7:fe:95:ff:8c:aa:ff:5f:54:cd:08:d4:de:fd:
    b3:da:82:3a:19:c9:d1:1d:46:a2:6c:5b:89:73:64:4b:06:e2:
    72:65:d9:76:30:05:ab:2a:e4:5f:a9:6a:21:06:9e:04:54:d4:
    31:72:36:4b:96:a7:86:e7:ea:9b:39:6a:2f:56:d3:4e:c0:6b:
    b2:42:db:26:00:7f:43:dd:a8:b7:22:d0:63:d9:59:e4:db:42:
    b4:43:80:91:44:8c:29:12:18:50:65:a5:c2:e7:26:16:e9:1b:
    4d:4e:06:22:40:5f:40:c4:04:6d:a9:bc:43:8a:3f:3c:d8:c2:
    9c:14:63:eb:f3:3f:68:6f:6c:d9:33:b6:d0:bf:c7:45:0b:b5:
    dc:a4:0b:9b:3d:1b:dd:1d:6b:66:72:c7:4f:27:78:cb:23:bd:
    ea:c2:33:be:0c:c1:64:54:8f:58:76:bf:fa:64:db:7d:b0:13:
    fe:46:f0:44:9a:d8:a9:22:8b:10:a1:a9:dd:97:fc:b5:30:40:
    33:7a:77:c4:42:98:1b:48:8b:24:78:02:df:bb:0c:24:84:65:
    40:36:9a:f1:de:b9:4f:96:9c:b0:af:90:58:48:fe:fa:f6:db:
    96:be:1d:32:bc:6b:cf:83:a1:c9:7b:25:22:db:0c:d4:fa:c3:
    75:aa:a8:f2:63:71:1d:6e:b2:69:3a:92:97:27:b7:53:68:62:
    df:40:1f:9b:fd:e3:fb:51:79:09:82:2b:27:ea:96:c6:89:dc:
    94:45:76:b5:27:10:c1:c9

┌──(root㉿kali)-[~/myCA]
└─# openssl genrsa -out ~/myCA/intermediateCA/private/intermediate.key.pem 4096

┌──(root㉿kali)-[~/myCA]
└─# chmod 400 ~/myCA/intermediateCA/private/intermediate.key.pem

┌──(root㉿kali)-[~/myCA]
└─# openssl req -config openssl_intermediate.cnf -key ~/myCA/intermediateCA/private/intermediate.key.pem -new -sha2
```



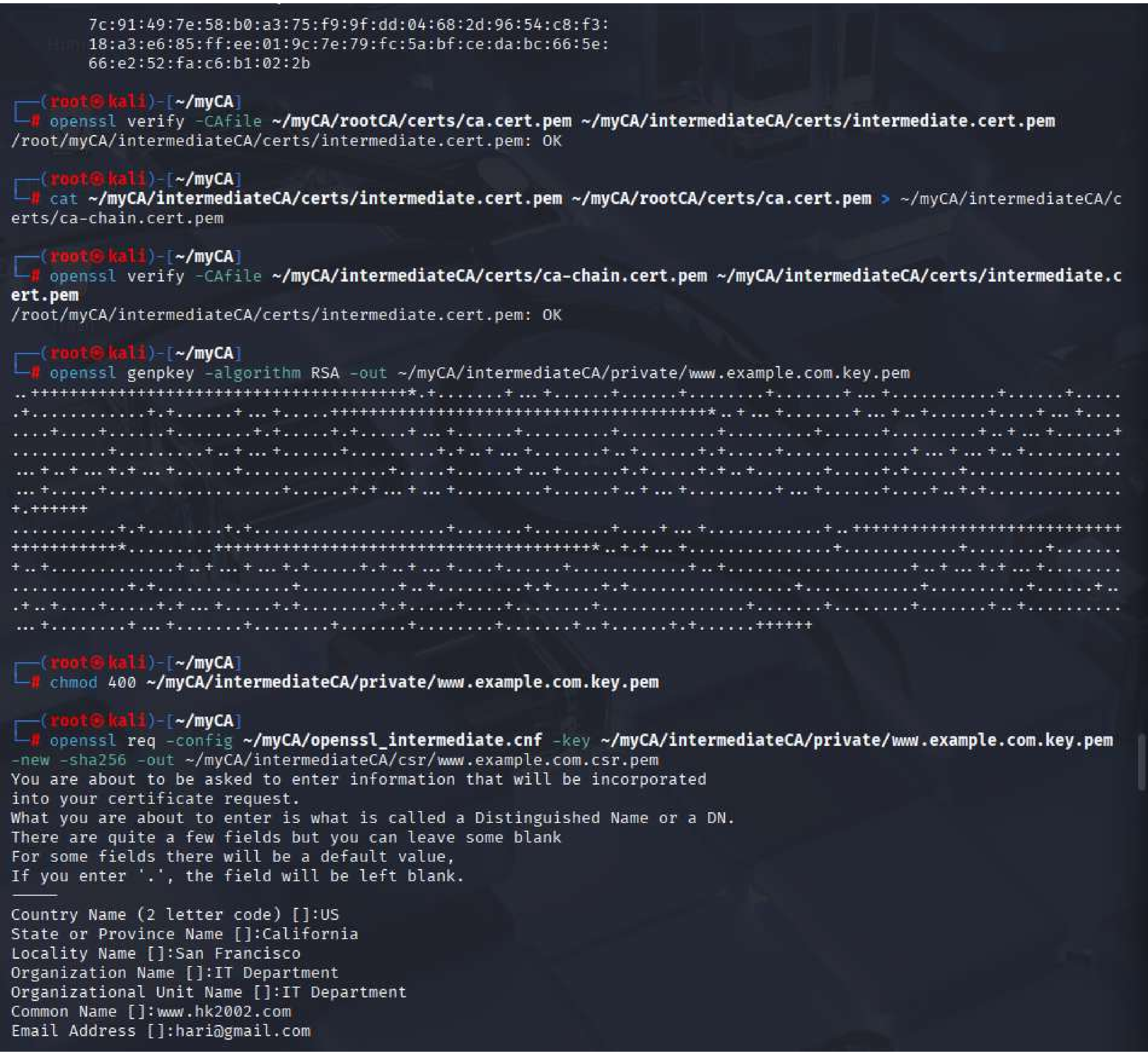
```
┌──(root㉿kali)-[~/myCA]
└─# openssl req -config openssl_intermediate.cnf -key ~/myCA/intermediateCA/private/intermediate.key.pem -new -sha2
56 -out ~/myCA/intermediateCA/certs/intermediate.csr.pem -subj "/C=US/ST=California/L=San Francisco/O=Example Corp/
OU=IT Department/CN=Intermediate CA"

┌──(root㉿kali)-[~/myCA]
└─# openssl ca -config openssl_root.cnf -extensions v3_intermediate_ca -days 3650 -notext -md sha256 -in ~/myCA/int
ermediateCA/certs/intermediate.csr.pem -out ~/myCA/intermediateCA/certs/intermediate.cert.pem
Using configuration from openssl_root.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0×1000)
        Validity
            Not Before: Sep 10 11:59:27 2025 GMT
            Not After : Sep  8 11:59:27 2035 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            organizationName          = Example Corp
            organizationalUnitName    = IT Department
            commonName                = Intermediate CA
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                8B:95:FC:F4:93:6A:C7:34:B1:E6:08:DB:F6:33:C4:23:48:D3:10:60
            X509v3 Authority Key Identifier:
                A2:0F:7A:C4:57:C7:E9:A3:93:16:4C:37:04:0C:7B:0E:7C:BE:7A:EA
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Sep  8 11:59:27 2035 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated

┌──(root㉿kali)-[~/myCA]
└─# chmod 444 ~/myCA/intermediateCA/certs/intermediate.cert.pem

┌──(root㉿kali)-[~/myCA]
└─# # cat ~/myCA/rootCA/index.txt
V 330503082700Z 1000 unknown /C=US/ST=California/O=Example Corp/OU=IT Department/CN=Intermediate CA
V: command not found

┌──(root㉿kali)-[~/myCA]
└─# # cat ~/myCA/rootCA/index.txt

┌──(root㉿kali)-[~/myCA]
└─# cat>~/myCA/rootCA/index.txt
V 330503082700Z 1000 unknown /C=US/ST=California/O=Example Corp/OU=IT Department/CN=Intermediate CA
```



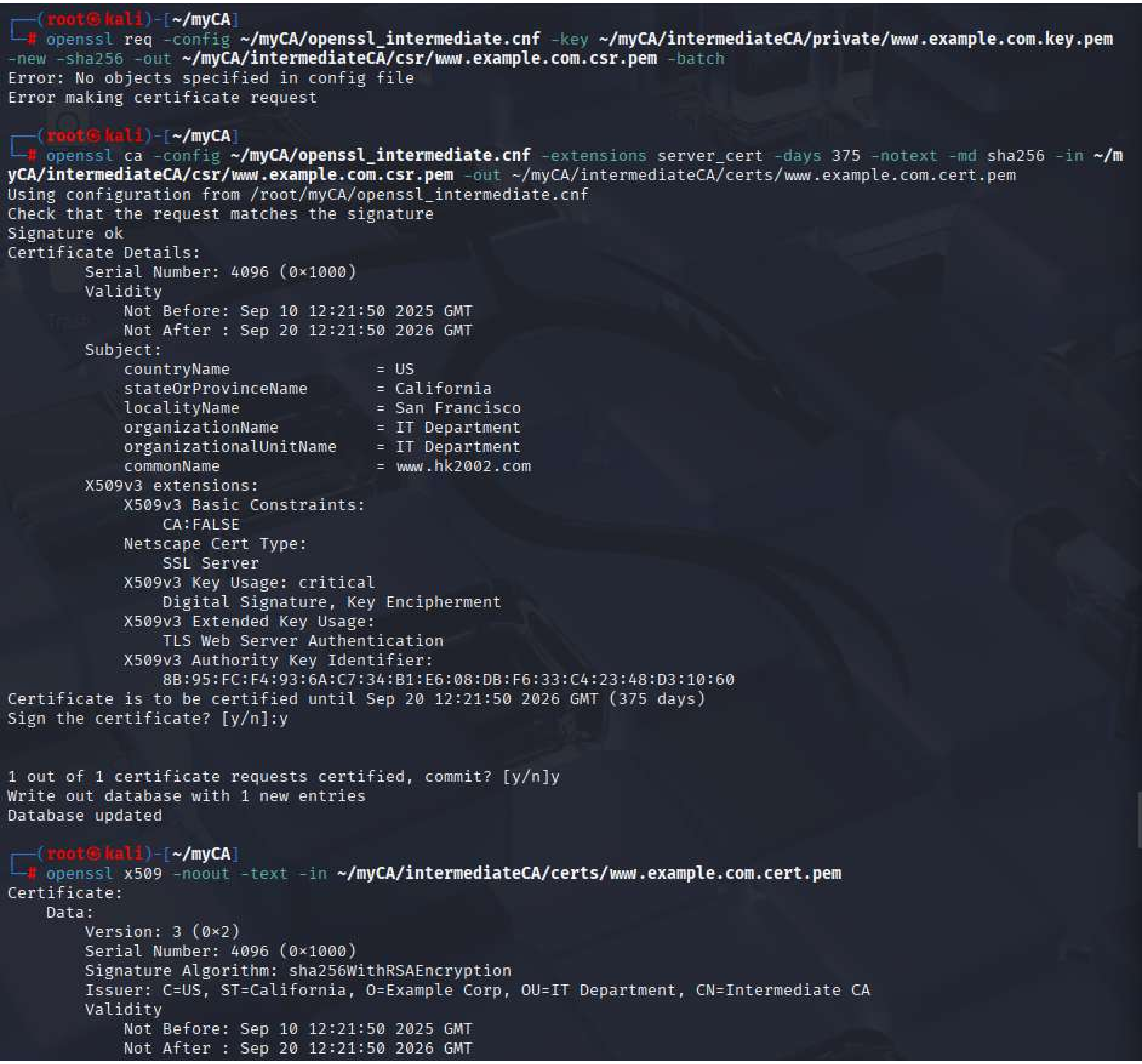
```
└─# # cat ~/myCA/rootCA/index.txt

┌──(root㉿kali)-[~/myCA]
└─# cat>~/myCA/rootCA/index.txt
V 330503082700Z 1000 unknown /C=US/ST=California/O=Example Corp/OU=IT Department/CN=Intermediate CA

┌──(root㉿kali)-[~/myCA]
└─# # cat ~/myCA/rootCA/index.txt

┌──(root㉿kali)-[~/myCA]
└─# cat ~/myCA/rootCA/index.txt
V 330503082700Z 1000 unknown /C=US/ST=California/O=Example Corp/OU=IT Department/CN=Intermediate CA

┌──(root㉿kali)-[~/myCA]
└─# openssl x509 -noout -text -in ~/myCA/intermediateCA/certs/intermediate.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, L=San Francisco, O=Example Corp, OU=IT Department, CN=Root CA
        Validity
            Not Before: Sep 10 11:59:27 2025 GMT
            Not After : Sep  8 11:59:27 2035 GMT
        Subject: C=US, ST=California, O=Example Corp, OU=IT Department, CN=Intermediate CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:92:f3:2a:fd:42:3f:e4:dd:0c:16:5f:3a:aa:cc:
                    93:16:f5:f1:a3:77:5d:a6:b2:fc:42:d6:ba:fc:2b:
                    cc:3b:78:0b:98:6f:6f:e0:84:39:e7:52:fa:86:29:
                    42:e4:5d:5b:ae:6a:52:06:58:7b:93:63:fe:5f:b9:
                    ed:8e:9d:64:30:15:cd:47:a7:e1:19:87:9f:3d:a5:
                    18:f2:3f:73:17:7b:81:0f:2f:67:af:bf:89:d5:0a:
                    62:8d:c3:7b:08:13:ff:02:b1:36:84:7e:ef:91:b2:
                    2b:93:07:b1:cc:2b:73:6f:61:31:ff:8b:cd:d7:a1:
                    b9:44:f4:a3:bf:ce:41:7e:83:d9:f0:d7:83:6d:b5:
                    3a:cd:2c:2b:f0:ba:16:5d:01:9c:b1:44:26:17:b5:
                    16:2e:4a:a5:25:da:8d:49:5c:98:1a:70:10:7c:b5:
                    2a:2f:dc:39:52:8f:03:55:2c:4e:b6:d5:92:e8:62:
                    a7:1c:4b:ec:1e:02:c8:e8:cb:bd:5c:7e:c4:fa:4b:
                    53:6c:71:35:e6:7e:25:29:6c:b7:b5:93:6a:48:d7:
                    b5:e1:7c:af:fc:05:fd:24:4e:0d:4e:ed:54:c0:4b:
                    8e:d2:ae:af:92:18:70:51:2b:0f:2c:49:79:ae:24:
                    57:7d:78:90:be:20:e2:96:33:40:9b:0b:85:c4:ae:
                    a7:cc:53:a6:4e:1d:62:96:ea:e9:c1:95:ac:79:8b:
                    42:c3:60:a1:ba:4a:a8:0f:70:59:f2:7e:15:c2:6c:
                    94:46:a6:a7:cc:c6:08:82:35:0a:a5:a9:df:26:a3:
                    a2:a5:a7:95:8e:10:08:d3:fe:43:a9:b2:58:88:75:
                    7f:7c:9d:34:47:70:bc:c4:10:53:50:80:f5:d0:86:
                    ed:af:f4:1c:d6:d3:6b:5d:48:9c:ea:8c:fc:ee:7d:
                    0a:52:84:5f:34:30:a6:69:e0:8a:c0:33:11:78:23:
                    5a:a3:0f:b9:c1:75:95:ef:01:dd:d8:22:56:f8:2b:
```



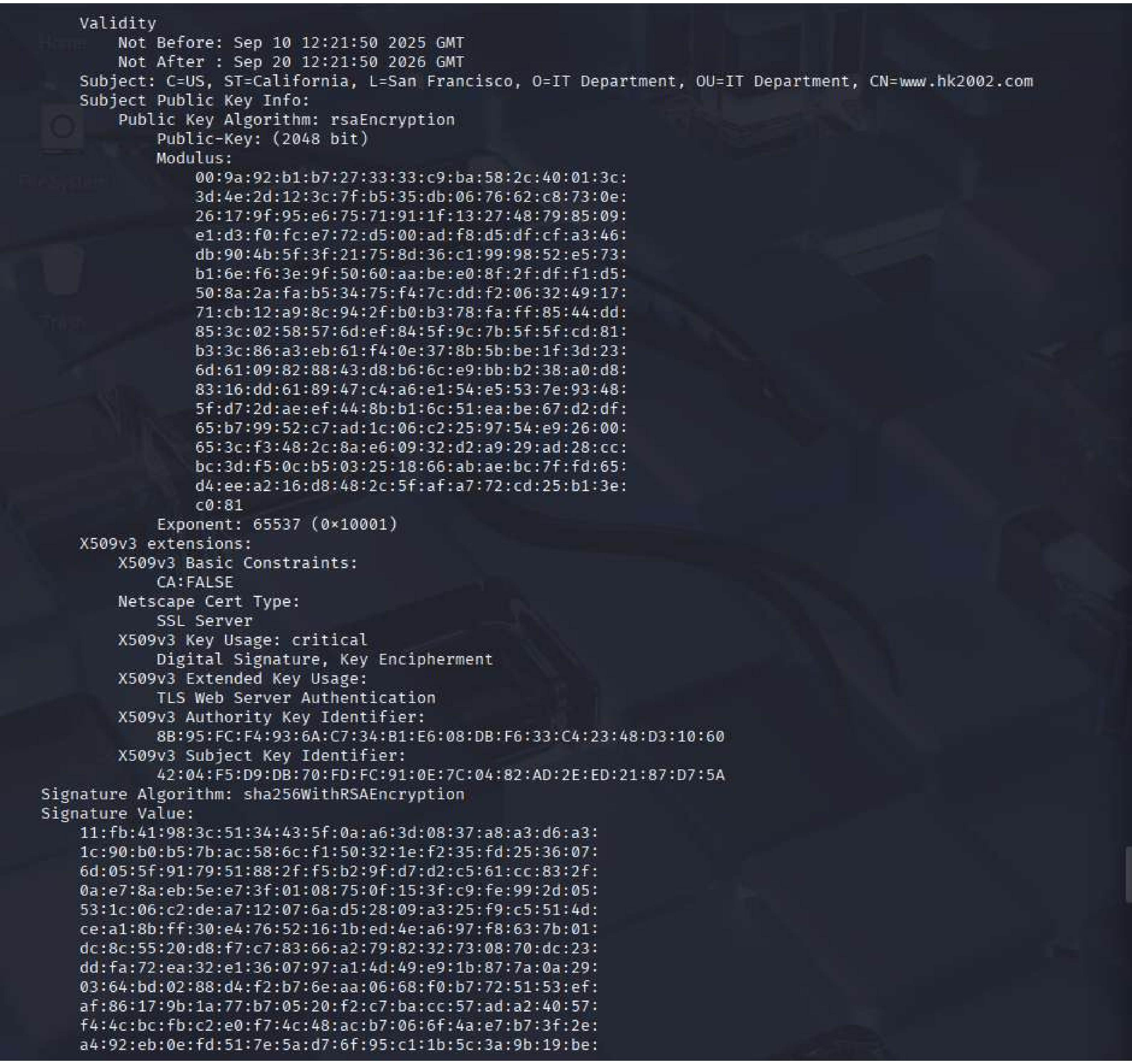
```
                    94:46:a6:a7:cc:c6:08:82:35:0a:a5:a9:df:26:a3:
                    a2:a5:a7:95:8e:10:08:d3:fe:43:a9:b2:58:88:75:
                    7f:7c:9d:34:47:70:bc:c4:10:53:50:80:f5:d0:86:
                    ed:af:f4:1c:d6:d3:6b:5d:48:9c:ea:8c:fc:ee:7d:
                    0a:52:84:5f:34:30:a6:69:e0:8a:c0:33:11:78:23:
                    5a:a3:0f:b9:c1:75:95:ef:01:dd:d8:22:56:f8:2b:
                    1a:b8:c0:16:46:72:c7:d5:27:fa:ef:5a:fe:1b:01:
                    79:a0:66:4a:fe:77:d7:5d:18:c7:3e:f7:cc:bf:d7:
                    15:d6:f5:9e:ff:0b:90:92:f8:cc:b7:a8:e0:99:45:
                    da:c9:10:4c:1b:cf:db:32:ef:7f:eb:5c:45:3a:29:
                    5e:93:02:7b:10:96:ec:f8:24:e6:68:7b:a4:60:c5:
                    e1:9f:ab:fa:c2:4b:aa:5b:a3:da:44:16:75:0e:7f:
                    9b:cd:a4:77:4b:f0:86:b3:3a:41:a5:e4:5c:aa:ac:
                    97:45:03:97:6b:a0:b9:5a:eb:2d:5e:38:78:ea:2f:
                    68:dd:c3:46:a5:c6:64:0a:da:a5:f1:39:5a:35:6f:
                    ff:4b:b1
                Exponent: 65537 (0×10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                8B:95:FC:F4:93:6A:C7:34:B1:E6:08:DB:F6:33:C4:23:48:D3:10:60
            X509v3 Authority Key Identifier:
                A2:0F:7A:C4:57:C7:E9:A3:93:16:4C:37:04:0C:7B:0E:7C:BE:7A:EA
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        42:dc:be:1f:6e:31:7f:2c:a5:ff:bb:65:54:42:34:d8:84:cc:
        06:2d:3d:95:fa:20:b3:0c:f1:f7:e9:d3:4a:32:55:38:88:4b:
        d7:c6:0a:b6:d5:5c:a0:03:28:31:bc:84:44:5e:f2:5c:4a:21:
        06:fb:01:f9:d5:cf:9b:bb:58:da:35:92:5b:37:ef:a2:49:32:
        d4:2f:d6:1c:78:61:5d:dc:7e:b6:26:50:54:f2:26:91:5d:1d:
        84:b1:10:c1:f9:1e:98:3a:3d:08:ee:11:b8:76:2a:5f:7f:4a:
        7a:ce:1c:df:6c:81:a1:b9:4f:36:bd:9a:5a:86:b9:aa:71:c2:
        87:60:02:4f:ff:32:4d:46:01:22:a0:2e:50:f2:7f:a1:69:9f:
        78:1e:61:c1:04:da:e0:c6:31:b7:a4:cd:87:41:7e:dd:3a:3d:
        60:31:01:bd:2d:01:2a:46:f1:31:eb:2a:7e:a2:11:df:4e:a4:
        11:cf:3f:ea:ca:14:45:19:4a:09:a4:90:94:b5:92:38:a0:7d:
        50:f5:e9:22:bc:30:17:2a:6d:04:3c:b2:be:8c:70:ad:33:59:
        6d:98:b4:27:aa:5b:15:7a:f6:57:1d:ef:1f:33:d3:67:2d:90:
        ea:25:ad:92:a8:df:ea:48:80:2b:ca:cb:19:ca:7f:b2:62:3f:
        90:5a:99:ad:c7:e1:a1:69:f0:d9:d6:69:6c:b6:d2:89:be:cf:
        04:0e:0d:34:93:f3:4d:c3:43:05:6c:3d:09:82:a5:31:9d:04:
        0e:d8:83:b5:fb:82:2f:97:aa:ea:f9:d7:44:74:4a:df:fd:35:
        f4:56:07:d1:69:98:df:f6:01:8b:d3:2b:67:ba:9c:83:e3:cf:
        6e:aa:12:05:02:60:ab:cc:77:98:81:01:57:67:6a:64:84:ab:
        5e:0a:61:ab:99:02:55:18:fd:87:07:2a:87:09:43:a1:ba:27:
        66:b9:65:63:2c:13:76:84:38:fb:32:60:22:ee:bb:5f:8a:95:
        40:57:42:6a:0b:f3:71:83:bc:2b:20:de:aa:7b:4e:05:24:cb:
        d0:09:09:ce:27:48:ba:8c:6f:41:b6:dc:63:3f:10:90:ca:95:
        dd:27:2d:30:ea:c5:44:b1:8f:28:a9:95:0c:85:33:4f:f5:2f:
        5e:fe:40:a5:83:f3:43:21:34:0a:d5:da:23:58:e7:7c:3f:46:
        85:51:c5:af:e2:7f:71:8d:d1:b0:c1:a9:4b:7c:13:63:a2:bb:
```



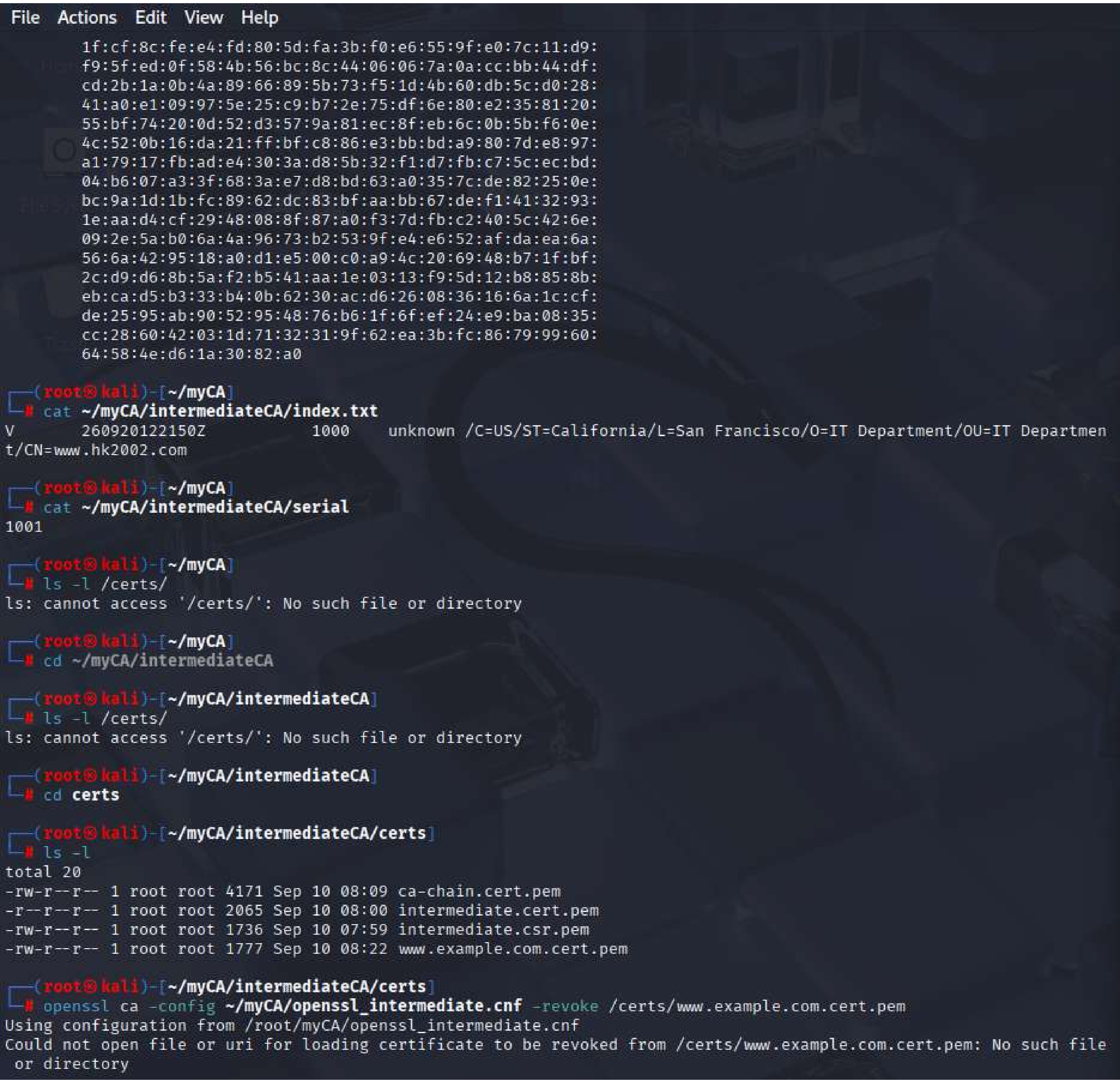
```
        7c:91:49:7e:58:b0:a3:75:f9:9f:dd:04:68:2d:96:54:c8:f3:
        18:a3:e6:85:ff:ee:01:9c:7e:79:fc:5a:bf:ce:da:bc:66:5e:
        66:e2:52:fa:c6:b1:02:2b

┌──(root㉿kali)-[~/myCA]
└─# openssl verify -CAfile ~/myCA/rootCA/certs/ca.cert.pem ~/myCA/intermediateCA/certs/intermediate.cert.pem
/root/myCA/intermediateCA/certs/intermediate.cert.pem: OK

┌──(root㉿kali)-[~/myCA]
└─# cat ~/myCA/intermediateCA/certs/intermediate.cert.pem ~/myCA/rootCA/certs/ca.cert.pem > ~/myCA/intermediateCA/c
erts/ca-chain.cert.pem

┌──(root㉿kali)-[~/myCA]
└─# openssl verify -CAfile ~/myCA/intermediateCA/certs/ca-chain.cert.pem ~/myCA/intermediateCA/certs/intermediate.c
ert.pem
/root/myCA/intermediateCA/certs/intermediate.cert.pem: OK

┌──(root㉿kali)-[~/myCA]
└─# openssl genpkey -algorithm RSA -out ~/myCA/intermediateCA/private/www.example.com.key.pem
..+++++++++++++++++++++++++++++++++++++++*.+........+...+......+......+.........+.......+...+...........+......+.....
.+............+.+......+...+.....++++++++++++++++++++++++++++++++++++++++*..+...+.......+...+..+......+....+...+....
....+....+......+.........+.+.....+.+.....+...+......+.........+.........+..........+.........+.......+..+...+.......+
..........+.........+..+...+......+.........+.+..+...+.......+..+.......+.+.....+............+...+...+..+..........
...+..+...+.+...+......+...............+.....+......+...+......+.+......+.+..+.......+.....+.+.....+................
...+......+...................+......+.+...+...+.........+......+..+...+..........+...+......+....+..+.+..............
+.++++++
..........+.+........+.+.....................+.......+.......+....+...+............+..++++++++++++++++++++++++++++
+++++++++++*.........++++++++++++++++++++++++++++++++++++++++*..+.+...+...............+...........+........+.......
+..+............+..+...+...+.+.....+.+..+...+....+.......+..+............+..+...+.+...+........
...........+.+..............+.........+..+..........+.+........+...........+.........+........+.......+..
.+..+....+.....+.+...+.....+.+..........+.+.....+....+..........+.........+..........+.........+..+...........
...+.........+...+.......+.........+.......+.......+..+......+.+......++++++

┌──(root㉿kali)-[~/myCA]
└─# chmod 400 ~/myCA/intermediateCA/private/www.example.com.key.pem

┌──(root㉿kali)-[~/myCA]
└─# openssl req -config ~/myCA/openssl_intermediate.cnf -key ~/myCA/intermediateCA/private/www.example.com.key.pem
-new -sha256 -out ~/myCA/intermediateCA/csr/www.example.com.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) []:US
State or Province Name []:California
Locality Name []:San Francisco
Organization Name []:IT Department
Organizational Unit Name []:IT Department
Common Name []:www.hk2002.com
Email Address []:hari@gmail.com
```



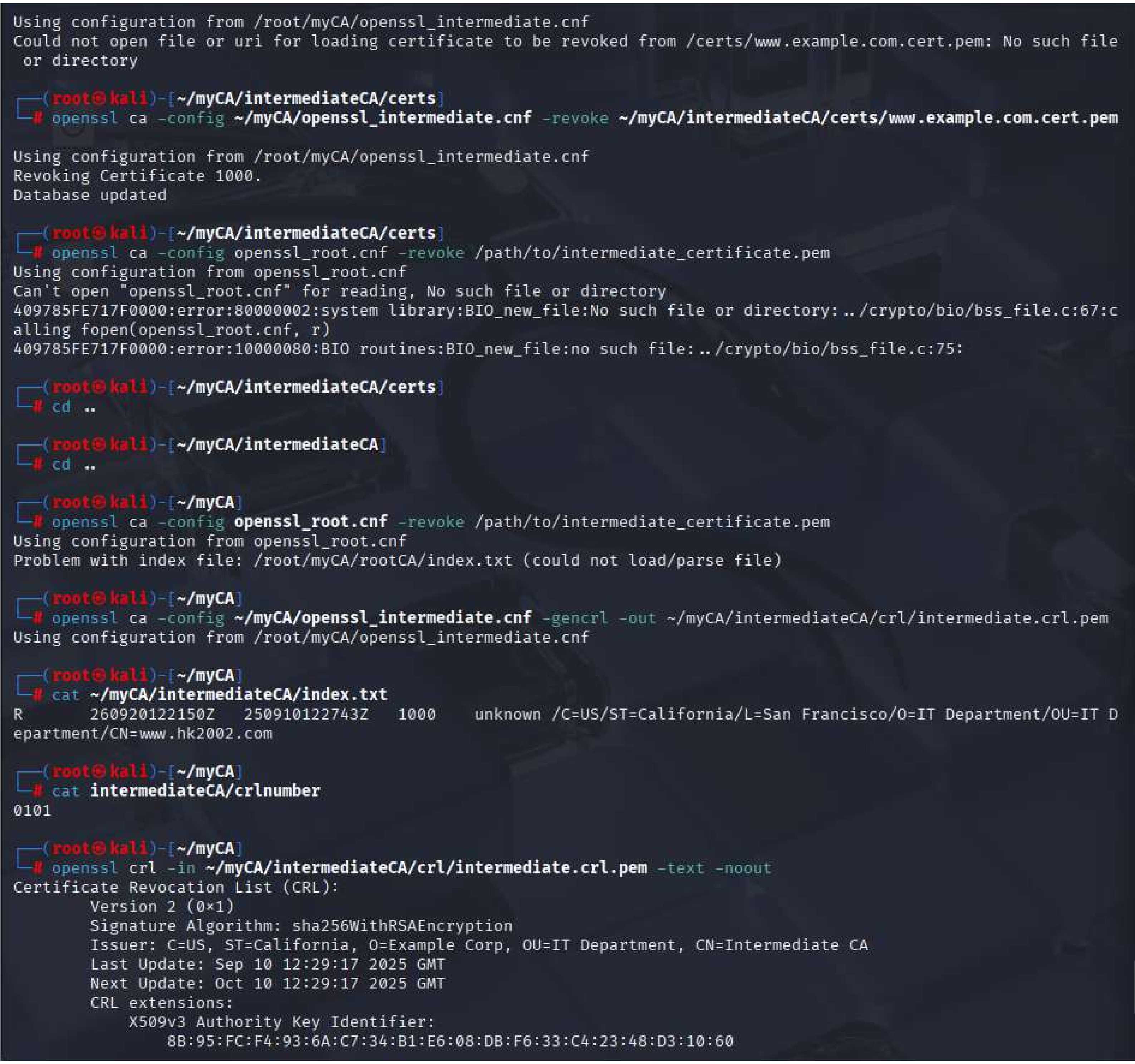
```
┌──(root㉿kali)-[~/myCA]
└─# openssl req -config ~/myCA/openssl_intermediate.cnf -key ~/myCA/intermediateCA/private/www.example.com.key.pem
-new -sha256 -out ~/myCA/intermediateCA/csr/www.example.com.csr.pem -batch
Error: No objects specified in config file
Error making certificate request

┌──(root㉿kali)-[~/myCA]
└─# openssl ca -config ~/myCA/openssl_intermediate.cnf -extensions server_cert -days 375 -notext -md sha256 -in ~/m
yCA/intermediateCA/csr/www.example.com.csr.pem -out ~/myCA/intermediateCA/certs/www.example.com.cert.pem
Using configuration from /root/myCA/openssl_intermediate.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0×1000)
        Validity
            Not Before: Sep 10 12:21:50 2025 GMT
            Not After : Sep 20 12:21:50 2026 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            localityName              = San Francisco
            organizationName          = IT Department
            organizationalUnitName    = IT Department
            commonName                = www.hk2002.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Authority Key Identifier:
                8B:95:FC:F4:93:6A:C7:34:B1:E6:08:DB:F6:33:C4:23:48:D3:10:60
Certificate is to be certified until Sep 20 12:21:50 2026 GMT (375 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Database updated

┌──(root㉿kali)-[~/myCA]
└─# openssl x509 -noout -text -in ~/myCA/intermediateCA/certs/www.example.com.cert.pem
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number: 4096 (0×1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, O=Example Corp, OU=IT Department, CN=Intermediate CA
        Validity
            Not Before: Sep 10 12:21:50 2025 GMT
            Not After : Sep 20 12:21:50 2026 GMT
```



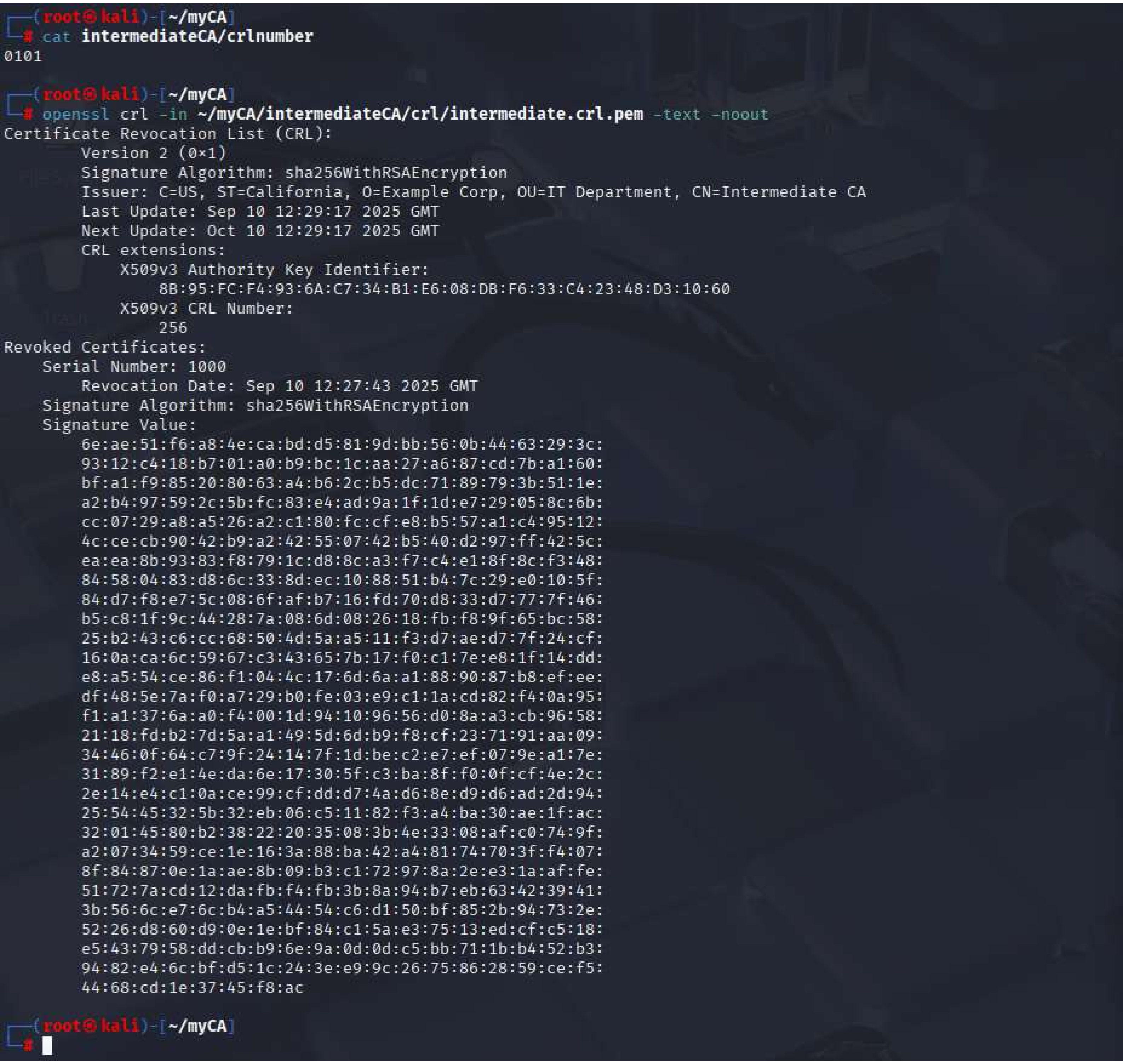
```
    Validity
        Not Before: Sep 10 12:21:50 2025 GMT
        Not After : Sep 20 12:21:50 2026 GMT
    Subject: C=US, ST=California, L=San Francisco, O=IT Department, OU=IT Department, CN=www.hk2002.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:9a:92:b1:b7:27:33:33:c9:ba:58:2c:40:01:3c:
                3d:4e:2d:12:3c:7f:b5:35:db:06:76:62:c8:73:0e:
                26:17:9f:95:e6:75:71:91:1f:13:27:48:79:85:09:
                e1:d3:f0:fc:e7:72:d5:00:ad:f8:d5:df:cf:a3:46:
                db:90:4b:5f:3f:21:75:8d:36:c1:99:98:52:e5:73:
                b1:6e:f6:3e:9f:50:60:aa:be:e0:8f:2f:df:f1:d5:
                50:8a:2a:fa:b5:34:75:f4:7c:dd:f2:06:32:49:17:
                71:cb:12:a9:8c:94:2f:b0:b3:78:fa:ff:85:44:dd:
                85:3c:02:58:57:6d:ef:84:5f:9c:7b:5f:5f:cd:81:
                b3:3c:86:a3:eb:61:f4:0e:37:8b:5b:be:1f:3d:23:
                6d:61:09:82:88:43:d8:b6:6c:e9:bb:b2:38:a0:d8:
                83:16:dd:61:89:47:c4:a6:e1:54:e5:53:7e:93:48:
                5f:d7:2d:ae:ef:44:8b:b1:6c:51:ea:be:67:d2:df:
                65:b7:99:52:c7:ad:1c:06:c2:25:97:54:e9:26:00:
                65:3c:f3:48:2c:8a:e6:09:32:d2:a9:29:ad:28:cc:
                bc:3d:f5:0c:b5:03:25:18:66:ab:ae:bc:7f:fd:65:
                d4:ee:a2:16:d8:48:2c:5f:af:a7:72:cd:25:b1:3e:
                c0:81
            Exponent: 65537 (0×10001)
    X509v3 extensions:
        X509v3 Basic Constraints:
            CA:FALSE
        Netscape Cert Type:
            SSL Server
        X509v3 Key Usage: critical
            Digital Signature, Key Encipherment
        X509v3 Extended Key Usage:
            TLS Web Server Authentication
        X509v3 Authority Key Identifier:
            8B:95:FC:F4:93:6A:C7:34:B1:E6:08:DB:F6:33:C4:23:48:D3:10:60
        X509v3 Subject Key Identifier:
            42:04:F5:D9:DB:70:FD:FC:91:0E:7C:04:82:AD:2E:ED:21:87:D7:5A
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
    11:fb:41:98:3c:51:34:43:5f:0a:a6:3d:08:37:a8:a3:d6:a3:
    1c:90:b0:b5:7b:ac:58:6c:f1:50:32:1e:f2:35:fd:25:36:07:
    6d:05:5f:91:79:51:88:2f:f5:b2:9f:d7:d2:c5:61:cc:83:2f:
    0a:e7:8a:eb:5e:e7:3f:01:08:75:0f:15:3f:c9:fe:99:2d:05:
    53:1c:06:c2:de:a7:12:07:6a:d5:28:09:a3:25:f9:c5:51:4d:
    ce:a1:8b:ff:30:e4:76:52:16:1b:ed:4e:a6:97:f8:63:7b:01:
    dc:8c:55:20:d8:f7:c7:83:66:a2:79:82:32:73:08:70:dc:23:
    dd:fa:72:ea:32:e1:36:07:97:a1:4d:49:e9:1b:87:7a:0a:29:
    03:64:bd:02:88:d4:f2:b7:6e:aa:06:68:f0:b7:72:51:53:ef:
    af:86:17:9b:1a:77:b7:05:20:f2:c7:ba:cc:57:ad:a2:40:57:
    f4:4c:bc:fb:c2:e0:f7:4c:48:ac:b7:06:6f:4a:e7:b7:3f:2e:
    a4:92:eb:0e:fd:51:7e:5a:d7:6f:95:c1:1b:5c:3a:9b:19:be:
```



```
        1f:cf:8c:fe:e4:fd:80:5d:fa:3b:f0:e6:55:9f:e0:7c:11:d9:
        f9:5f:ed:0f:58:4b:56:bc:8c:44:06:06:7a:0a:cc:bb:44:df:
        cd:2b:1a:0b:4a:89:66:89:5b:73:f5:1d:4b:60:db:5c:d0:28:
        41:a0:e1:09:97:5e:25:c9:b7:2e:75:df:6e:80:e2:35:81:20:
        55:bf:74:20:0d:52:d3:57:9a:81:ec:8f:eb:6c:0b:5b:f6:0e:
        4c:52:0b:16:da:21:ff:bf:c8:86:e3:bb:bd:a9:80:7d:e8:97:
        a1:79:17:fb:ad:e4:30:3a:d8:5b:32:f1:d7:fb:c7:5c:ec:bd:
        04:b6:07:a3:3f:68:3a:e7:d8:bd:63:a0:35:7c:de:82:25:0e:
        bc:9a:1d:1b:fc:89:62:dc:83:bf:aa:bb:67:de:f1:41:32:93:
        1e:aa:d4:cf:29:48:08:8f:87:a0:f3:7d:fb:c2:40:5c:42:6e:
        09:2e:5a:b0:6a:4a:96:73:b2:53:9f:e4:e6:52:af:da:ea:6a:
        56:6a:42:95:18:a0:d1:e5:00:c0:a9:4c:20:69:48:b7:1f:bf:
        2c:d9:d6:8b:5a:f2:b5:41:aa:1e:03:13:f9:5d:12:b8:85:8b:
        eb:ca:d5:b3:33:b4:0b:62:30:ac:d6:26:08:36:16:6a:1c:cf:
        de:25:95:ab:90:52:95:48:76:b6:1f:6f:ef:24:e9:ba:08:35:
        cc:28:60:42:03:1d:71:32:31:9f:62:ea:3b:fc:86:79:99:60:
        64:58:4e:d6:1a:30:82:a0

┌──(root㉿kali)-[~/myCA]
└─# cat ~/myCA/intermediateCA/index.txt
V       260920122150Z           1000    unknown /C=US/ST=California/L=San Francisco/O=IT Department/OU=IT Departmen
t/CN=www.hk2002.com

┌──(root㉿kali)-[~/myCA]
└─# cat ~/myCA/intermediateCA/serial
1001

┌──(root㉿kali)-[~/myCA]
└─# ls -l /certs/
ls: cannot access '/certs/': No such file or directory

┌──(root㉿kali)-[~/myCA]
└─# cd ~/myCA/intermediateCA

┌──(root㉿kali)-[~/myCA/intermediateCA]
└─# ls -l /certs/
ls: cannot access '/certs/': No such file or directory

┌──(root㉿kali)-[~/myCA/intermediateCA]
└─# cd certs

┌──(root㉿kali)-[~/myCA/intermediateCA/certs]
└─# ls -l
total 20
-rw-r--r-- 1 root root 4171 Sep 10 08:09 ca-chain.cert.pem
-r--r--r-- 1 root root 2065 Sep 10 08:00 intermediate.cert.pem
-rw-r--r-- 1 root root 1736 Sep 10 07:59 intermediate.csr.pem
-rw-r--r-- 1 root root 1777 Sep 10 08:22 www.example.com.cert.pem

┌──(root㉿kali)-[~/myCA/intermediateCA/certs]
└─# openssl ca -config ~/myCA/openssl_intermediate.cnf -revoke /certs/www.example.com.cert.pem
Using configuration from /root/myCA/openssl_intermediate.cnf
Could not open file or uri for loading certificate to be revoked from /certs/www.example.com.cert.pem: No such file
 or directory
```



```
Using configuration from /root/myCA/openssl_intermediate.cnf
Could not open file or uri for loading certificate to be revoked from /certs/www.example.com.cert.pem: No such file
 or directory

┌──(root㉿kali)-[~/myCA/intermediateCA/certs]
└─# openssl ca -config ~/myCA/openssl_intermediate.cnf -revoke ~/myCA/intermediateCA/certs/www.example.com.cert.pem

Using configuration from /root/myCA/openssl_intermediate.cnf
Revoking Certificate 1000.
Database updated

┌──(root㉿kali)-[~/myCA/intermediateCA/certs]
└─# openssl ca -config openssl_root.cnf -revoke /path/to/intermediate_certificate.pem
Using configuration from openssl_root.cnf
Can't open "openssl_root.cnf" for reading, No such file or directory
409785FE717F0000:error:80000002:system library:BIO_new_file:No such file or directory:../crypto/bio/bss_file.c:67:c
alling fopen(openssl_root.cnf, r)
409785FE717F0000:error:10000080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:75:

┌──(root㉿kali)-[~/myCA/intermediateCA/certs]
└─# cd ..

┌──(root㉿kali)-[~/myCA/intermediateCA]
└─# cd ..

┌──(root㉿kali)-[~/myCA]
└─# openssl ca -config openssl_root.cnf -revoke /path/to/intermediate_certificate.pem
Using configuration from openssl_root.cnf
Problem with index file: /root/myCA/rootCA/index.txt (could not load/parse file)

┌──(root㉿kali)-[~/myCA]
└─# openssl ca -config ~/myCA/openssl_intermediate.cnf -gencrl -out ~/myCA/intermediateCA/crl/intermediate.crl.pem
Using configuration from /root/myCA/openssl_intermediate.cnf

┌──(root㉿kali)-[~/myCA]
└─# cat ~/myCA/intermediateCA/index.txt
R       260920122150Z   250910122743Z   1000    unknown /C=US/ST=California/L=San Francisco/O=IT Department/OU=IT D
epartment/CN=www.hk2002.com

┌──(root㉿kali)-[~/myCA]
└─# cat intermediateCA/crlnumber
0101

┌──(root㉿kali)-[~/myCA]
└─# openssl crl -in ~/myCA/intermediateCA/crl/intermediate.crl.pem -text -noout
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, O=Example Corp, OU=IT Department, CN=Intermediate CA
        Last Update: Sep 10 12:29:17 2025 GMT
        Next Update: Oct 10 12:29:17 2025 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                8B:95:FC:F4:93:6A:C7:34:B1:E6:08:DB:F6:33:C4:23:48:D3:10:60
```



```
┌──(root㉿kali)-[~/myCA]
└─# cat intermediateCA/crlnumber
0101

┌──(root㉿kali)-[~/myCA]
└─# openssl crl -in ~/myCA/intermediateCA/crl/intermediate.crl.pem -text -noout
Certificate Revocation List (CRL):
        Version 2 (0×1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=California, O=Example Corp, OU=IT Department, CN=Intermediate CA
        Last Update: Sep 10 12:29:17 2025 GMT
        Next Update: Oct 10 12:29:17 2025 GMT
        CRL extensions:
            X509v3 Authority Key Identifier: 
                8B:95:FC:F4:93:6A:C7:34:B1:E6:08:DB:F6:33:C4:23:48:D3:10:60
            X509v3 CRL Number: 
                256
Revoked Certificates:
    Serial Number: 1000
        Revocation Date: Sep 10 12:27:43 2025 GMT
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        6e:ae:51:f6:a8:4e:ca:bd:d5:81:9d:bb:56:0b:44:63:29:3c:
        93:12:c4:18:b7:01:a0:b9:bc:1c:aa:27:a6:87:cd:7b:a1:60:
        bf:a1:f9:85:20:80:63:a4:b6:2c:b5:dc:71:89:79:3b:51:1e:
        a2:b4:97:59:2c:5b:fc:83:e4:ad:9a:1f:1d:e7:29:05:8c:6b:
        cc:07:29:a8:a5:26:a2:c1:80:fc:cf:e8:b5:57:a1:c4:95:12:
        4c:ce:cb:90:42:b9:a2:42:55:07:42:b5:40:d2:97:ff:42:5c:
        ea:ea:8b:93:83:f8:79:1c:d8:8c:a3:f7:c4:e1:8f:8c:f3:48:
        84:58:04:83:d8:6c:33:8d:ec:10:88:51:b4:7c:29:e0:10:5f:
        84:d7:f8:e7:5c:08:6f:af:b7:16:fd:70:d8:33:d7:77:7f:46:
        b5:c8:1f:9c:44:28:7a:08:6d:08:26:18:fb:f8:9f:65:bc:58:
        25:b2:43:c6:cc:68:50:4d:5a:a5:11:f3:d7:ae:d7:7f:24:cf:
        16:0a:ca:6c:59:67:c3:43:65:7b:17:f0:c1:7e:e8:1f:14:dd:
        e8:a5:54:ce:86:f1:04:4c:17:6d:6a:a1:88:90:87:b8:ef:ee:
        df:48:5e:7a:f0:a7:29:b0:fe:03:e9:c1:1a:cd:82:f4:0a:95:
        f1:a1:37:6a:a0:f4:00:1d:94:10:96:56:d0:8a:a3:cb:96:58:
        21:18:fd:b2:7d:5a:a1:49:5d:6d:b9:f8:cf:23:71:91:aa:09:
        34:46:0f:64:c7:9f:24:14:7f:1d:be:c2:e7:ef:07:9e:a1:7e:
        31:89:f2:e1:4e:da:6e:17:30:5f:c3:ba:8f:f0:0f:cf:4e:2c:
        2e:14:e4:c1:0a:ce:99:cf:dd:d7:4a:d6:8e:d9:d6:ad:2d:94:
        25:54:45:32:5b:32:eb:06:c5:11:82:f3:a4:ba:30:ae:1f:ac:
        32:01:45:80:b2:38:22:20:35:08:3b:4e:33:08:af:c0:74:9f:
        a2:07:34:59:ce:1e:16:3a:88:ba:42:a4:81:74:70:3f:f4:07:
        8f:84:87:0e:1a:ae:8b:09:b3:c1:72:97:8a:2e:e3:1a:af:fe:
        51:72:7a:cd:12:da:fb:f4:fb:3b:8a:94:b7:eb:63:42:39:41:
        3b:56:6c:e7:6c:b4:a5:44:54:c6:d1:50:bf:85:2b:94:73:2e:
        52:26:d8:60:d9:0e:1e:bf:84:c1:5a:e3:75:13:ed:cf:c5:18:
        e5:43:79:58:dd:cb:b9:6e:9a:0d:0d:c5:bb:71:1b:b4:52:b3:
        94:82:e4:6c:bf:d5:1c:24:3e:e9:9c:26:75:86:28:59:ce:f5:
        44:68:cd:1e:37:45:f8:ac

┌──(root㉿kali)-[~/myCA]
└─# 
```