

1. Untuk memahami cara kerja Public Key Infrastructure (PKI), Anda dapat untuk menggunakan Linux (Ubuntu/Kali) untuk mengerjakan tugas melakukan Self Sign Certificate dengan mengenerate CA dan sertifikat server sendiri.

- ### Langkah-langkahnya

- jawab :

[illegible]

Membuat Certificate untuk 2 Domain berikut:

1. studiindependen2023.com
2. [namaanda]-lab2023.com (sesuaikan dengan nama anda masing masing) :

Membuat key nya :

```
(asyrof@asyrof)-[~/cert]
$ openssl genrsa --aes128 -out studiindependen2024.com.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

(asyrof@asyrof)-[~/cert]
$ openssl genrsa --aes128 -out asyrof-lab2024.com.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Generate public/private key pair untuk masing masing domain dan Cara melihat key yang masih terenskripsi :

```
(asyrof@asyrof)-[~/cert]
$ cat asyrof-lab2024.com.key
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFNTBfBgkqhkiG9w0BBQ0wUjAxBgkqhkiG9w0BBQwwJAQQkgI83b8rwp/i3MfQ
kxmYIwICCAAwDAYIKoZIhvcNAQkFADAdBglgghkgBZQMEAAQIEEE3m0d0LyhACC6hK
DA1ufoAEggTQOV3s0SX3JCCs00yYNZCanADLTpA9j6Zj7IB3mtIFyXefKjCrVIS
xT9Ev9DY8xK7Bj0knWh4Iq0yKde7BeTsbT1DoF02/+bTaYb6X6ZxpBVGNJVivTfJ
vGloVdn8UpmTXfiRBF5HiY+fzLcRlk5VQa7MJvIHn9u+hNykryprdp37clzgCaee
j/Zm282jMzvtY70c5RQbTLBipa04CjVrhhrBu1jP7GIAYL1T8QE0rFmx0BP4viNY
bXASnqfEp2R2eTKAql1rSPmPP09uY4qSzcX4cS3Wwi7ypzLFFf9KGRCRwTiVGvZK
H41B9Z2ZqDuSTCDQeWUVkF397X23uM6LAdLcQg8o/+nfUaRXlj+9Lhqor+6/KeE08
07h9yAytURWvsILqknstdFmadvdcM2FtvQfRYpesg9hhyAHXlbXVMbm7Ghsxgg37
gifUGno3gwYW3Qj0BzGtE0XpW1x8y56Y2NHge2/DAZ/+JZmyRoEH0JW850efThve
fIVGIgYtDSzqdXGYMmEW0TSPi58MLFDPmbML1bWdkzWu1yLGPGL1CV2k1cbuhwEO
nWjkzRupXldErJZ+asB+RioPjFzSUHZ64qjodfTQR42dFHBvET8jA0bD1AjjfBFo
+krw/8hPt3qOp1hjJ2E+b+xSc/YAbLxo+TFbDcoRv11QbB9wmlqwEvtJDSbhRqag
DEAE5W8050K42Q1WPsdCnchmgkn3ou9sDTNa21C3C1WI47ljhP0LcMsWu4fSiyl1
t2jzqcGWUL8g5gv098wTGAzi364nANC0VEVUStk000gUWll7F8QLevpNQL7UratV
C6PhiEKPYKDrRGICHONYwTgfn+zAe+ZkBaECfXvBc5Jwh+kNGsIGMwXbinl9yY2Y
ix7nQxcRczH6zhDBkGUBVR+LLV+Ni1ph65MhBUXBGYKpvCqqBs6/4DWHzhW8I1om
pp19Qn92QuBfnolxiPrLYukr8Nna+9UpGw8wLU20C8eX817+qkdPtIi0KE+f4ja
p4b+xTHCC+6dDyhnqpBeLUg+VJIgo0vB9AGnkuVlz6kA4o3c6nVraC1CdQoP9JCe
WgN0+PuMiVXl+i2DLvi0b94NfrmvPFxtYEBzM0ZV6FNAU/xu5S3u0YTguJCvYD24
kg00ZMJavV2Aw2YUIVInf0NU3pCQ+NL23C6IRV7pQvd/wiREZiV12Z/+T2pWK5Cd
ffaEXueVTnEeebNtlyTBfibcs1sldfmo8Y57V+1QX1rflTm6KNTULLc+W3KraPZZ
Q8w67i6TVMgLc3SAB6QJmshnvnC06HCveAXrXb4a7vs06sX364DdLXMODXZLacCx
SQIe85yFuYubE6QmsYHbVgavCehlSOSET2GL3zuQUbBS7mUcr4tdBy15hG7BeqVW
v51eWF7/gWZuisyzC6sy0Lbv+jnPu5rJRiyyUiA4R0uXR0w58DTSqr87QTGtp7ai
Ph7c8bw9Y60IViV++sRWCEG3qlvve6N5sKbTL2Y/oU6sE1TI+dAL9boip5ayJrE
xPMGievWfuiJQ/SB20LZcxcUY94RgV68hsTNAIQFgX354Wo0/Wvj3PsK7dIBE60Z
EfOV96YD+KC1N13H6SuyCfLCGLm6/L05WAewXWRBzSPGQYU3FdrnK7o=
-----END ENCRYPTED PRIVATE KEY-----

(asyrof@asyrof)-[~/cert]
$
```

Melihat certificate nya :

Studiindependen2024.com.key

```
(asyrof@asyrof) [~/cert]
$ openssl rsa -in studiiindependen2024.com.key -text
Enter pass phrase for studiiindependen2024.com.key:
Private-Key: (2048 bit, 2 primes)
modulus:
 00:b1:c0:cc:2f:90:7d:78:07:e8:c6:5c:0f:05:1a:
89:df:f0:52:ed:dc:c8:98:06:7f:46:72:ff:7e:8f:
b8:fb:83:95:9a:72:05:42:0c:01:ab:d5:e6:72:89:
4a:26:5f:b7:eb:47:21:3b:86:38:ea:43:c1:d2:60:
4d:64:36:07:a4:af:03:40:25:2d:13:15:ce:58:a1:
b0:bf:4d:b3:80:83:01:05:4a:42:39:64:76:dc:ac:
9b:2c:02:6d:33:92:a1:88:9a:35:b9:4a:7c:64:2d:
d3:7b:f5:1d:55:29:b1:c3:ad:45:6f:64:ea:96:7e:
06:88:3c:6f:22:a0:68:16:0b:4c:05:62:fb:49:46:
37:d1:0e:9c:84:6b:88:e9:b3:2c:c2:c3:82:21:0a:
be:ec:f0:80:dd:bf:00:a6:3d:1d:05:92:78:b3:e8:
09:4e:d7:14:5c:11:9e:52:6f:82:76:9d:f9:ee:19:
15:12:50:1b:d5:95:39:f1:9e:12:1f:6a:b4:8d:8c:
69:b0:06:c2:2e:7b:65:f5:d2:92:90:61:fb:7b:fa:
30:04:98:8d:82:53:d2:11:02:7d:7a:80:74:de:d2:
5e:71:9b:70:1b:16:d6:15:af:09:25:0e:bd:0e:5c:
2c:fa:12:bf:7a:e2:a2:20:50:8a:48:e8:49:f2:01:
3b:69
publicExponent: 65537 (0x10001)
privateExponent:
 54:05:88:de:f0:e3:46:4e:a4:0a:e3:68:58:a7:ff:
45:32:27:a9:dd:03:9a:cd:e5:6f:84:f6:b3:99:f7:
7c:38:2b:a3:f5:a0:63:1a:2e:37:0e:10:74:d2:6d:
90:cf:0d:0e:73:5c:73:99:12:1d:36:33:0f:a1:02:
e4:1c:20:07:c9:cc:75:0d:3d:9d:b8:60:86:07:c4:
16:e1:81:38:7d:74:45:8e:60:f8:65:13:44:63:78:
a3:d8:6f:cb:01:84:46:a0:72:45:a8:3e:5d:52:46:
15:e1:7a:e0:8f:29:5e:8f:f0:af:64:d9:f8:92:10:
bf:64:25:ba:4d:ed:75:81:4d:aa:3f:21:cf:7a:cb:
9b:c1:42:f3:7c:fd:6a:c7:fa:7d:06:39:ea:77:e3:
51:fb:bf:b6:95:c0:7f:b4:99:d5:86:4b:52:db:38:
95:76:61:98:07:3b:43:2e:0f:99:a6:08:55:38:26:
ac:d0:c6:9a:6d:59:d9:26:b3:70:3a:b7:53:d0:f9:
00:2b:d9:2c:15:1b:9d:5d:03:15:11:f8:2f:bf:12:
e5:8c:f3:af:08:82:29:35:a2:4d:89:ad:40:33:52:
fd:db:27:5d:e3:3a:9e:9b:1d:2d:83:53:73:b4:
27:b7:26:0a:4c:b8:31:e5:57:de:ae:94:75:1b:08:
4b
prime1:
 00:f0:aa:96:df:62:31:d0:49:c1:d7:b8:62:8b:9c:
21:89:ff:d8:38:1d:03:52:35:80:c7:24:2e:e8:2c:
89:c9:eb:cc:67:e4:12:6e:4b:8b:79:1a:56:a5:d6:
e1:bc:88:56:a2:01:20:b5:d3:d9:20:7a:bb:ca:f6:
4f:e6:58:de:29:c3:be:83:f6:3a:4e:57:10:6d:af:
0c:c0:45:00:90:de:0e:69:da:2e:f0:4a:7b:50:7e:
9f:d7:b7:1b:f9:3c:19:17:55:29:ea:1a:27:6e:81:
5e:f3:54:12:d9:5c:31:f3:d9:bf:57:5d:8a:ae:44:
c2:bf:20:c7:4c:26:7d:c3:ab
```

Asyrof-lab2024.com.key

```
(asyrof@asyrof) [~/cert]
$ openssl rsa -in asyrof-lab2024.com.key -text
Enter pass phrase for asyrof-lab2024.com.key:
Private-Key: (2048 bit, 2 primes)
modulus:
 00:d6:0e:d1:73:13:de:e8:7f:e1:86:d6:3a:e8:28:
b5:f1:ad:6e:cc:ab:c3:e0:6c:88:c1:56:34:a7:8b:
1d:99:c5:0b:00:01:69:59:de:0e:bd:c5:5f:3b:cf:
80:87:bd:07:8d:a5:44:78:fe:93:ff:e5:94:76:3f:
42:17:99:27:1c:4f:cc:df:73:af:92:32:ef:c7:a9:
6c:6b:63:35:16:97:ab:92:dd:05:45:33:57:a2:80:
18:29:bc:85:80:35:9b:90:85:1f:89:5b:d3:13:ba:
f1:25:59:f3:68:b4:02:2c:88:88:7f:73:b4:35:69:
ab:58:cc:ad:4a:28:62:38:e3:25:26:62:e5:78:c1:
53:07:5e:a7:c5:67:81:9d:37:bd:02:d1:01:f7:70:
1a:c3:73:7f:a4:ff:d2:44:df:3e:e0:04:f9:a6:b6:
e6:32:90:65:fa:bb:11:5c:28:d8:3f:80:17:47:e8:
0c:43:c5:69:8a:83:b8:a7:3f:9b:c5:66:60:98:28:
98:39:ca:2d:bd:f8:1b:08:75:87:31:ad:d9:92:10:
d0:1a:97:64:38:9b:c3:f7:f5:8c:31:37:9b:85:32:
68:60:6b:e3:fd:f0:84:ff:93:24:5c:1e:97:4a:b7:
b7:a6:1b:07:51:00:6c:7a:a3:96:81:4b:2a:f6:3b:
0b:cf
publicExponent: 65537 (0x10001)
privateExponent:
 10:65:32:d3:b3:f4:ec:82:9c:52:88:91:70:7b:6b:
1c:27:62:dc:d8:57:23:6c:62:0e:74:e7:89:8c:55:
3d:be:e2:e3:22:e3:35:2d:40:9c:76:6e:9f:3f:d0:
77:6a:6f:6c:00:f9:92:a4:3a:7a:6c:d4:dc:8d:bc:
7b:de:e6:28:fb:fa:69:84:61:db:e5:27:8a:77:c6:
99:c9:ba:7a:3a:d9:bb:0b:a4:be:07:d0:5c:33:a0:
26:2a:38:b6:23:8f:ab:c2:6b:dc:f3:24:8d:56:a7:
3b:c0:d2:57:a0:59:fe:46:8d:8b:3d:8b:28:55:7f:
4d:f3:8c:b3:a9:0e:2f:8f:1f:c0:f5:c4:a7:72:f1:
cf:23:0f:ad:4d:69:4e:ce:82:95:15:6d:83:fe:51:
2e:4a:58:53:db:fd:64:59:9c:46:16:4d:a5:30:80:
5c:26:a7:0a:2c:d7:fd:30:66:b6:b3:a3:c5:4d:fc:
7a:87:c8:d5:c4:8e:46:4f:2b:71:ff:74:c4:9c:41:
f2:83:82:c3:c1:22:9d:8a:50:33:97:bd:c6:96:4e:
b9:3b:ac:c0:5e:ec:08:0b:99:0a:40:3d:79:04:c3:
83:cd:1c:93:ae:80:13:e4:21:be:29:98:f1:f0:3b:
8d:09:33:ec:33:4d:d4:99:72:52:ad:3e:36:77:0f:
c1
prime1:
 00:f5:31:72:a5:f0:da:ce:aa:94:63:a9:56:4c:08:
e8:94:31:a2:1f:1c:d5:4f:ca:64:bd:67:2e:4f:09:
28:83:c3:8a:40:d5:56:fa:3c:70:0d:50:ef:65:c8:
d0:48:80:41:92:9e:40:0f:a2:26:1a:43:e7:1d:68:
6a:e5:e3:ba:22:ea:35:7a:5a:c5:04:d3:72:c8:34:
be:ce:81:47:e5:20:ea:33:dd:51:a3:86:53:62:a7:
cd:e8:c1:ac:27:9b:61:e7:75:5f:2b:57:89:8e:ac:
cc:33:ed:30:0d:8a:ed:65:ed:17:03:b9:0b:01:81:
f9:b4:83:ea:b9:da:6e:e1:21
```



Generate a Certificate Signing Request (CSR) untuk masing masing domain :

Domain studiindependen2024.com

```
(asyrof@asyrof)-[~/cert]
$ ls
asyrof-lab2024.com.key  ca.crt  ca.key  studiindependen2024.com.key

(asyrof@asyrof)-[~/cert]
$ ls -al
total 24
drwxrwxr-x  2 asyrof asyrof 4096 Nov  2 02:47 .
drwx----- 22 asyrof asyrof 4096 Nov  2 02:45 ..
-rw-----  1 asyrof asyrof 1886 Nov  2 02:47 asyrof-lab2024.com.key
-rw-r--r--  1 root  root   1513 Nov  2 02:38 ca.crt
-rw-----  1 root  root   1862 Nov  2 02:34 ca.key
-rw-----  1 asyrof asyrof 1886 Nov  2 02:46 studiindependen2024.com.key

(asyrof@asyrof)-[~/cert]
$ openssl req -new -key studiindependen2024.com.key -out studiindependen2024.com.csr
Enter pass phrase for studiindependen2024.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:D.I.Yogyakarta
Locality Name (eg, city) []:Sleman
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTDI
Organizational Unit Name (eg, section) []:Teknik Komputer
Common Name (e.g. server FQDN or YOUR name) []:studiindependen2024.com
Email Address []:pengerjadikamenrider@gmail.com

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

Domain Asyrof-lab2024.com

```
(asyrof@asyrof)-[~/cert]
$ openssl req -new -key asyrof-lab2024.com.key -out asyrof-lab2024.com.csr
Enter pass phrase for asyrof-lab2024.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:D.I.Yogyakarta
Locality Name (eg, city) []:Sleman
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTDI
Organizational Unit Name (eg, section) []:Teknik Komputer
Common Name (e.g. server FQDN or YOUR name) []:asyrof-lab2024.com
Email Address []:pengerjadikamenrider@gmail.com

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

Generate Certificates dengan menggunakan CA yang sudah dibuat sebelumnya untuk masing masing csr domain :

Buat folder baru :

```
kalinux_asyrof [Running] - Oracle VM VirtualBox
File Actions Edit View Help
[asyrof@asyrof]-[~]
└─$ mkdir tugas
[asyrof@asyrof]-[~]
└─$ cd tugas
[asyrof@asyrof]-[~/tugas]
└─$ ls
[asyrof@asyrof]-[~/tugas]
└─$ mkdir demoCA
[asyrof@asyrof]-[~/tugas]
└─$ ls
ls: command not found
[asyrof@asyrof]-[~/tugas]
└─$
[asyrof@asyrof]-[~/tugas]
└─$ ls
Command 'ls' not found, did you mean:
command 'l's' from deb sleuthkit
command 'l's' from deb coreutils
command 'f's' from deb sleuthkit
command 's'l's' from deb heimdal-multidev
command 's'l's' from deb s'l's
command 's'l's' from deb libnet-amazon-s3-tools-perl
command 's'l's' from deb sleuthkit
command 's's' from deb sssreport
command 'o's' from deb speech-tools
command 'd's' from deb bacula-sd
command 's'r's' from deb srs
command 's'l's' from deb stool
command 's'l's' from deb s'l'sh
command 's's' from deb iproute2
command 'f's' from deb rustup
Try: sudo apt install <deb name>
[asyrof@asyrof]-[~/tugas]
└─$ ls
demoCA
[asyrof@asyrof]-[~/tugas]
└─$ cd demoCA
[asyrof@asyrof]-[~/tugas/demoCA]
└─$ mkdir newcerts
[asyrof@asyrof]-[~/tugas/demoCA]
└─$ touch serial
[asyrof@asyrof]-[~/tugas/demoCA]
└─$ touch index.txt
[asyrof@asyrof]-[~/tugas/demoCA]
└─$ ls -al
total 12
drwxrwxr-x 3 asyrof asyrof 4096 Nov  2 06:57 .
drwxrwxr-x 1 asyrof asyrof 4096 Nov  2 06:56 ..
-rw-rw-r-- 1 asyrof asyrof  0 Nov  2 06:57 index.txt
drwxrwxr-x 2 asyrof asyrof 4096 Nov  2 06:57 newcerts
-rw-rw-r-- 1 asyrof asyrof  0 Nov  2 06:57 serial
[asyrof@asyrof]-[~/tugas/demoCA]
```

Menyalin file openssl.cnf dari direktori /usr/lib/ssl/ ke direktori tugas :

```
(asyrof@asyrof)-[~/tugas]
└─$ cp /usr/lib/ssl/openssl.cnf .
(asyrof@asyrof)-[~/tugas]
└─$ ls
demoCA  openssl.cnf
```

```
(asyrof@asyrof)-[~/tugas]
└─$ ls
demoCA  openssl.cnf
```

Membuat sertifikat self-signed x509 beserta kunci private nya :

[illegible]

Membuat kunci privat RSA yang dienkripsi dengan algoritma AES-128 dan hasilnya disimpan dalam file studiindependen2024.com.key :

```
(asyrof@asyrof)-[~/tugas]
$ openssl genrsa --aes128 -out studiindependen2024.com.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

Buat sama untuk file Asyrof-lab2024.com.key :

```
(asyrof@asyrof)-[~/tugas]
$ openssl genrsa -aes128 -out asyrof-lab2024.com.key 2048
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
(asyrof@asyrof)-[~/tugas]
$ ls
asyrof-lab2024.com.key  ca.crt  ca.key  demoCA  openssl.cnf  studiindependen2024.com.key
```

Membuat CSR (Certificate Signing Request ) untuk domain studiindependen2024.com :

```
(asyrof@asyrof)-[~/tugas]
$ openssl req -new -key studiindependen2024.com.key -out studiindependen2024.com.csr --config openssl.cnf
Enter pass phrase for studiindependen2024.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:D.I.Yogyakarta
Locality Name (eg, city) []:Sleman
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTDI
Organizational Unit Name (eg, section) []:Teknik Komputer
Common Name (e.g. server FQDN or YOUR name) []:studiindependen2024.com
Email Address []:pengerjadikamenrider@gmail.com

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

Buat sama untuk domain Asyrof-lab2024.com :

```
(asyrof@asyrof)-[~/tugas]
$ openssl req -new -key asyrof-lab2024.com.key -out asyrof-lab2024.com.csr --config openssl.cnf
Enter pass phrase for asyrof-lab2024.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:ID
Locality Name (eg, city) []:D.I.Yogyakarta
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTDI
Organizational Unit Name (eg, section) []:Teknik KOMputer
Common Name (e.g. server FQDN or YOUR name) []:asyrof-lab2024.com
Email Address []:pengerjadikamenrider@gmail.com

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

```
(asyrof@asyrof)-[~/tugas]
$ ls
asyrof-lab2024.com.csr  asyrof-lab2024.com.key  ca.crt  ca.key  demoCA  openssl.cnf  studiindependen2024.com.csr  st
```

```
(asyrof@asyrof)-[~/tugas]
$ ls -al
total 52
drwxrwxr-x 3 asyrof asyrof 4096 Nov 2 07:10 .
drwx----- 23 asyrof asyrof 4096 Nov 2 06:55 ..
-rw-rw-r-- 1 asyrof asyrof 1094 Nov 2 07:10 asyrof-lab2024.com.csr
-rw----- 1 asyrof asyrof 1886 Nov 2 07:06 asyrof-lab2024.com.key
-rw-rw-r-- 1 asyrof asyrof 1513 Nov 2 07:04 ca.crt
-rw----- 1 asyrof asyrof 1862 Nov 2 07:03 ca.key
drwxrwxr-x 3 asyrof asyrof 4096 Nov 2 06:57 demoCA
-rw-r--r-- 1 asyrof asyrof 12550 Nov 2 06:59 openssl.cnf
-rw-rw-r-- 1 asyrof asyrof 1106 Nov 2 07:08 studiindependen2024.com.csr
-rw----- 1 asyrof asyrof 1886 Nov 2 07:05 studiindependen2024.com.key
```



Buat folder private di demoCA :

```
(asyrof@asyrof)-[~/tugas]
$ mkdir demoCA/private
```

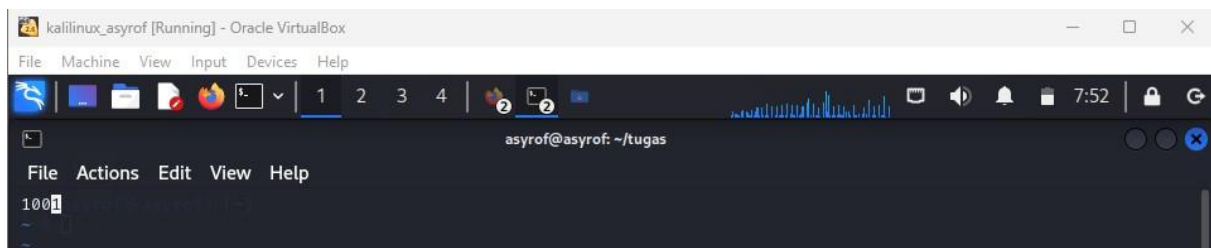
Menyalin isi dari file ca.key ke dalam file demoCA/private/cakey.pem :

```
(asyrof@asyrof)-[~/tugas]
$ cat ca.key > demoCA/private/cakey.pem
```

Openssl tidak bisa menemukan/membaca nomor serial yang diperlukan untuk sertifikat,jadi saya membuat nomor serial sendiri :

```
(asyrof@asyrof)-[~/tugas]
$ openssl ca -in studiindependen2024.com.csr -out studiindependen2024.com.crt -cert ca.crt keyfile ca.key -config openssl.cnf
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Unable to load number from ./demoCA/serial
40D7D8F6BD7F0000:error:06800096:asn1 encoding routines:a2i_ASN1_INTEGER:short line:../crypto/asn1/f_int.c:138:
error while loading serial number

(asyrof@asyrof)-[~/tugas]
$ vi demoCA/serial
```



Menandatangani permintaan sertifikat (CSR) dengan openssl (studiindependen2024.com) :

```
(asyrof@asyrof)-[~/tugas]
$ openssl ca -in studiindependen2024.com.csr -out studiindependen2024.com.crt -cert ca.crt -keyfile ca.key -config openssl.cnf

Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4096 (0x1000)
  Validity
    Not Before: Nov  2 11:39:10 2024 GMT
    Not After : Nov  2 11:39:10 2025 GMT
  Subject:
    countryName           = ID
    stateOrProvinceName   = D.I.Yogyakarta
    organizationName       = UTDI
    organizationalUnitName = Teknik Komputer
    commonName             = studiindependen2024.com
    emailAddress           = pengenjadikamenrider@gmail.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Subject Key Identifier:
      E3:B8:78:18:38:FE:6D:34:47:D7:60:0C:0D:EB:B9:27:55:FF:CD:99
    X509v3 Authority Key Identifier:
      59:6F:5C:36:A1:EA:EF:18:7E:04:A6:4E:99:6E:F4:27:AE:02:A6:C4
Certificate is to be certified until Nov  2 11:39:10 2025 GMT (365 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

(asyrof@asyrof)-[~/tugas]
$
```



Sertifikat dengan serial number yang saya inputkan :

```
(asyrof@asyrof)-[~/tugas/demoCA]
$ cd newcerts

(asyrof@asyrof)-[~/tugas/demoCA/newcerts]
$ ls
1000.pem

(asyrof@asyrof)-[~/tugas/demoCA/newcerts]
$ ls -al
total 16
drwxrwxr-x 2 asyrof asyrof 4096 Nov  2 07:39 .
drwxrwxr-x 4 asyrof asyrof 4096 Nov  2 07:52 ..
-rw-rw-r-- 1 asyrof asyrof 4646 Nov  2 07:39 1000.pem

(asyrof@asyrof)-[~/tugas/demoCA/newcerts]
$
```

Menandatangani permintaan sertifikat (CSR) dengan openssl (Asyrof-lab2024.com) :

```
(asyrof@asyrof)-[~/tugas]
$ openssl req -new -key asyrof-lab2024.com.key -out asyrof-lab2024.com.csr
Enter pass phrase for asyrof-lab2024.com.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:D.I.Yogyakarta
Locality Name (eg, city) []:Sleman
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UTDI
Organizational Unit Name (eg, section) []:Teknik Komputer
Common Name (e.g. server FQDN or YOUR name) []:asyrof-lab2024.com
Email Address []:pengenjadikamenrider@gmail.com

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

(asyrof@asyrof)-[~/tugas]
$ openssl ca -in asyrof-lab2024.com.csr -out asyrof-lab2024.com.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 4097 (0x1001)
  Validity
    Not Before: Nov  2 12:02:09 2024 GMT
    Not After : Nov  2 12:02:09 2025 GMT
  Subject:
    countryName           = ID
    stateOrProvinceName   = D.I.Yogyakarta
    organizationName       = UTDI
    organizationalUnitName = Teknik Komputer
    commonName             = asyrof-lab2024.com
    emailAddress           = pengenjadikamenrider@gmail.com
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Subject Key Identifier:
      B5:CC:C8:63:32:14:04:B9:81:E7:25:DF:F3:20:D7:47:BB:9F:76:8E
    X509v3 Authority Key Identifier:
      59:6F:5C:36:A1:EA:EF:18:7E:04:A6:4E:99:6E:F4:27:AE:02:A6:C4
Certificate is to be certified until Nov  2 12:02:09 2025 GMT (365 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

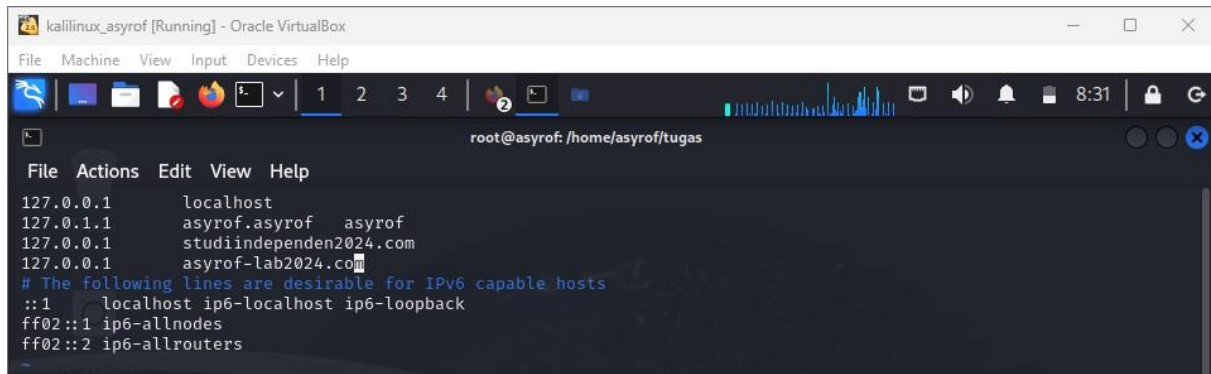
(asyrof@asyrof)-[~/tugas]
$
```

```
(asyrof@asyrof)-[~/tugas]
$ ls
asyrof-lab2024.com.crt  asyrof-lab2024.com.key  ca.key  openssl.cnf  studiindependen2024.com.csr
asyrof-lab2024.com.csr  ca.crt                  demoCA  studiindependen2024.com.crt  studiindependen2024.com.key

(asyrof@asyrof)-[~/tugas]
$
```

Mapping static di etc/host :

```
(root@asyrof)-[/home/asyrof/tugas]
# vi /etc/hosts
```



The screenshot shows a terminal window titled 'kalilinux\_asyrof [Running] - Oracle VirtualBox'. The terminal is running as root at the asyrof machine, in the directory /home/asyrof/tugas. The /etc/hosts file is open in a text editor, showing the following content:

```
File Actions Edit View Help
127.0.0.1      localhost
127.0.1.1      asyrof.asyrof  asyrof
127.0.0.1      studiindependen2024.com
127.0.0.1      asyrof-lab2024.co
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

Cek apakah sudah benar konfigurasnya dengan ping :

Studiindependen2024.com

```
(root@asyrof)-[/home/asyrof/tugas]
# ping studiindependen2024.com
PING studiindependen2024.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.127 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.059 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.028 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.053 ms
64 bytes from localhost (127.0.0.1): icmp_seq=7 ttl=64 time=0.050 ms
64 bytes from localhost (127.0.0.1): icmp_seq=8 ttl=64 time=0.047 ms
64 bytes from localhost (127.0.0.1): icmp_seq=9 ttl=64 time=0.047 ms
64 bytes from localhost (127.0.0.1): icmp_seq=10 ttl=64 time=0.059 ms
64 bytes from localhost (127.0.0.1): icmp_seq=11 ttl=64 time=0.061 ms
64 bytes from localhost (127.0.0.1): icmp_seq=12 ttl=64 time=0.048 ms
64 bytes from localhost (127.0.0.1): icmp_seq=13 ttl=64 time=0.048 ms
64 bytes from localhost (127.0.0.1): icmp_seq=14 ttl=64 time=0.056 ms
64 bytes from localhost (127.0.0.1): icmp_seq=15 ttl=64 time=0.059 ms
64 bytes from localhost (127.0.0.1): icmp_seq=16 ttl=64 time=0.068 ms
64 bytes from localhost (127.0.0.1): icmp_seq=17 ttl=64 time=0.074 ms
64 bytes from localhost (127.0.0.1): icmp_seq=18 ttl=64 time=0.047 ms
64 bytes from localhost (127.0.0.1): icmp_seq=19 ttl=64 time=0.061 ms
```

```
(root@asyrof)-[/home/asyrof/tugas]
# ping asyrof-lab2024.com
PING asyrof-lab2024.com (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.060 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.060 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.061 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.057 ms
^C
— asyrof-lab2024.com ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5114ms
rtt min/avg/max/mdev = 0.024/0.048/0.061/0.015 ms

(root@asyrof)-[/home/asyrof/tugas]
#
```

Mengaktifkan default ssl :

```
(root@asyrof)-[/etc/apache2/sites-enabled]
# cd ..

(root@asyrof)-[/etc/apache2]
# cd sites-available

(root@asyrof)-[/etc/apache2/sites-available]
# ls -al

total 20
drwxr-xr-x 2 root root 4096 Oct 25 13:09 ..
drwxr-xr-x 8 root root 4096 Oct 25 13:09 .
-rw-r--r-- 1 root root 2114 Oct  8 02:47 000-default.conf
-rw-r--r-- 1 root root 4573 Jul  7 09:26 default-ssl.conf

(root@asyrof)-[/etc/apache2/sites-available]
# a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
systemctl reload apache2
```

Navigasikan ke direktori sites-available apache2, direktori ini menyimpan virtual host untuk apache 2 termasuk file konfigurasi SSL :

```
File Actions Edit View Help
(asyrof@asyrof)-[~]
$ cd /etc/apache2/
```

```

(asyrof@asyrof)-[/etc/apache2]
$ cd sites-available

(asyrof@asyrof)-[/etc/apache2/sites-available]
$ ls
000-default.conf  default-ssl.conf

(asyrof@asyrof)-[/etc/apache2/sites-available]
$ ls -al
total 20
drwxr-xr-x 2 root root 4096 Nov  2 08:50 .
drwxr-xr-x 8 root root 4096 Oct 25 13:09 ..
-rw-r--r-- 1 root root 2114 Oct  8 02:47 000-default.conf
-rw-r--r-- 1 root root 4573 Jul  7 09:26 default-ssl.conf

```

Salin konfigurasi SSL default ke nama domain :

```

(asyrof@asyrof)-[/etc/apache2/sites-available]
$ sudo su
[sudo] password for asyrof:
(root@asyrof)-[/etc/apache2/sites-available]
# cp default-ssl.conf studiindependen2024.com-ssl.conf

(root@asyrof)-[/etc/apache2/sites-available]
# cp default-ssl.conf asyrof-lab2024.com-ssl.conf

```

Edit konfigurasi SSL untuk domain studiindependen2024.com seperti mengatur nama domain dan path sertifikat :

```

(root@asyrof)-[/etc/apache2/sites-available]
# vi studiindependen2024.com-ssl.conf

```

Masuk ke file konfigurasi ssl :



```
kalilinux_asyrof [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4 | 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100
root@asyrof: /etc/apache2/sites-available

File Actions Edit View Help

<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName studiindependen2024.com
    DocumentRoot /var/www/studiindependen2024

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

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

    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/studiindependen2024.com.crt
    SSLCertificateKeyFile /etc/ssl/private/studiindependen2024.com.key

    # Server Certificate Chain:
    # Point SSLCertificateChainFile at a file containing the
    # concatenation of PEM encoded CA certificates which form the
    # certificate chain for the server certificate. Alternatively
    # the referenced file can be the same as SSLCertificateFile
    # when the CA certificates are directly appended to the server
    # certificate for convinience.
    #SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt

    # Certificate Authority (CA):
    # Set the CA certificate verification path where to find CA
    # certificates for client authentication or alternatively one
    # huge file containing all of them (file must be PEM encoded)
    # Note: Inside SSLCACertificatePath you need hash symlinks
    # to point to the certificate files. Use the provided
    # Makefile to update the hash symlinks after changes.
    #SSLCACertificatePath /etc/ssl/certs/
    #SSLCACertificateFile /etc/apache2/ssl.crt/ca-bundle.crt

"studiindependen2024.com-ssl.conf" 101L, 4636B 5,0-1 Top
```

Menambahkan ServerName studiindependen2024.com dan letak DocumenRoot nya pada /var/www/studiindependen2024 :

```
<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName studiindependen2024.com
    DocumentRoot /var/www/studiindependen2024
```

Mengatur letak public key dan private key :

```
SSLCertificateFile /etc/ssl/certs/studiindependen2024.com.crt
SSLCertificateKeyFile /etc/ssl/private/studiindependen2024.com.key
```

Kembali ke direktori home dan mengakses tugas :

```
(root@asyrof)-[~] # cd /home
(root@asyrof)-[/home] # cd /home/asyrof
(root@asyrof)-[/home/asyrof] # cd tugas
(root@asyrof)-[/home/asyrof/tugas] # ls
asyrof-lab2024.com.crt  asyrof-lab2024.com.key  ca.key  openssl.cnf  studiindependen2024.com.csr
asyrof-lab2024.com.csr  ca.crt  demoCA  studiindependen2024.com.crt  studiindependen2024.com.key
```

Menyalin file sertifikat dan kunci :

```
(root@asyrof)-[/home/asyrof/tugas] # cp studiindependen2024.com.crt /etc/ssl/certs/
(root@asyrof)-[/home/asyrof/tugas] # cp studiindependen2024.com.key /etc/ssl/private/
```

Melihat daftar file konfigurasi dan mengaktifkan situs SSL :

```
(root@asyrof)-[/home/asyrof/tugas] # cd /etc/apache2/sites-available
(root@asyrof)-[/etc/apache2/sites-available] # ls
000-default.conf  asyrof-lab2024.com-ssl.conf  default-ssl.conf  studiindependen2024.com-ssl.conf
(root@asyrof)-[/etc/apache2/sites-available] # less studiindependen2024.com-ssl.conf
a2ensite studiindependen2024.com-ssl
Enabling site studiindependen2024.com-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
(root@asyrof)-[/etc/apache2/sites-available] # systemctl reload apache2
```

Memasukkan passphrase untuk ssl :

```
(root@asyrof)-[/etc/apache2/sites-available] #
Broadcast message from root@asyrof (Sun 2024-11-03 02:12:00 EST):

Password entry required for 'Enter passphrase for SSL/TLS keys for studiindependen2024.com:443 (RSA):' (PID 32015).
Please enter password with the systemd-tty-ask-password-agent tool.
Enter passphrase for SSL/TLS keys for studiindependen2024.com:443 (RSA):
(root@asyrof)-[/etc/apache2/sites-available] # systemctl reload apache2
Enter passphrase for SSL/TLS keys for studiindependen2024.com:443 (RSA): .....
```

Membuat folder studiindependen2024 :

```
(root@asyrof)-[/etc/apache2/sites-available] # cd /var/www
(root@asyrof)-[/var/www] # mkdir studiindependen2024
```

Membuat halaman utama file index.html :

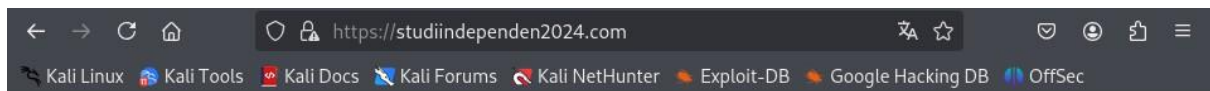
```
(root@asyrof)-[/var/www]
# vi index.html
```

```
root@asyrof: /var/www/studiindependen2024
File Actions Edit View Help
Selamat datang di studi independen 2024
```

Reload/restart apache2 lalu masuk ke web domain localhost studiindependen2024.com :

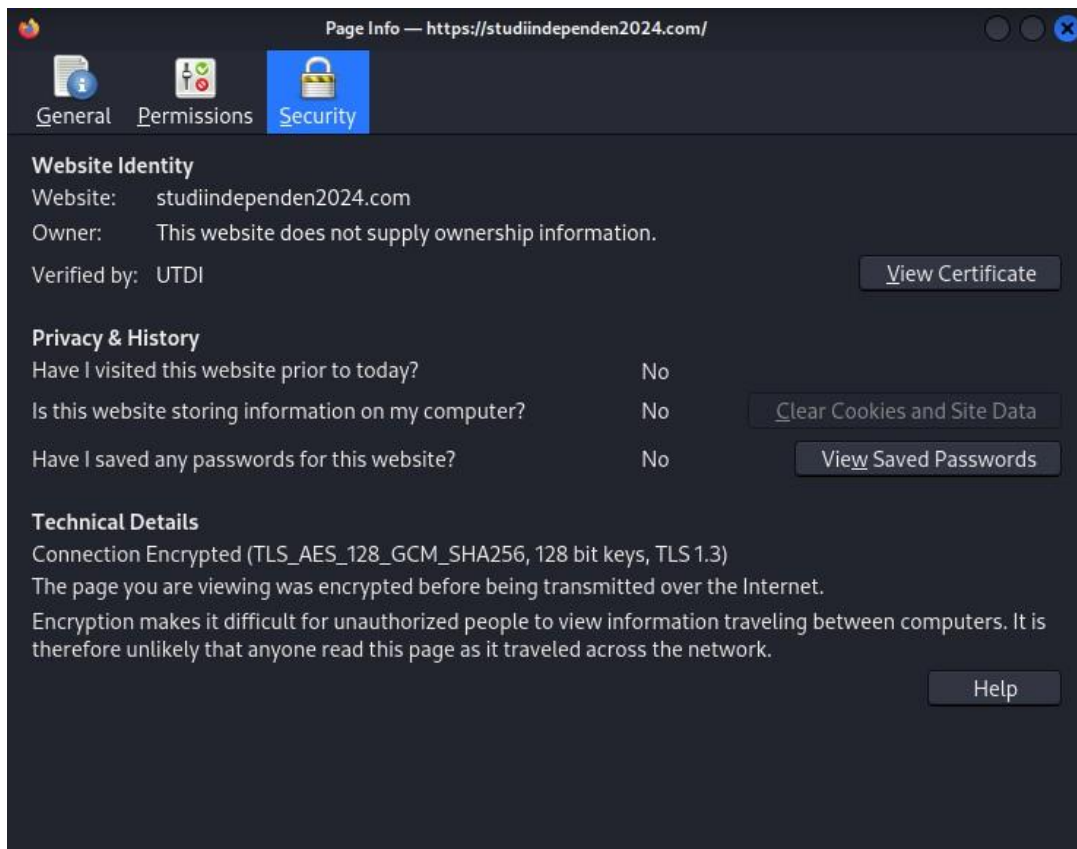
```
(root@asyrof)-[/var/www/studiindependen2024]
# service apache2 reload
```

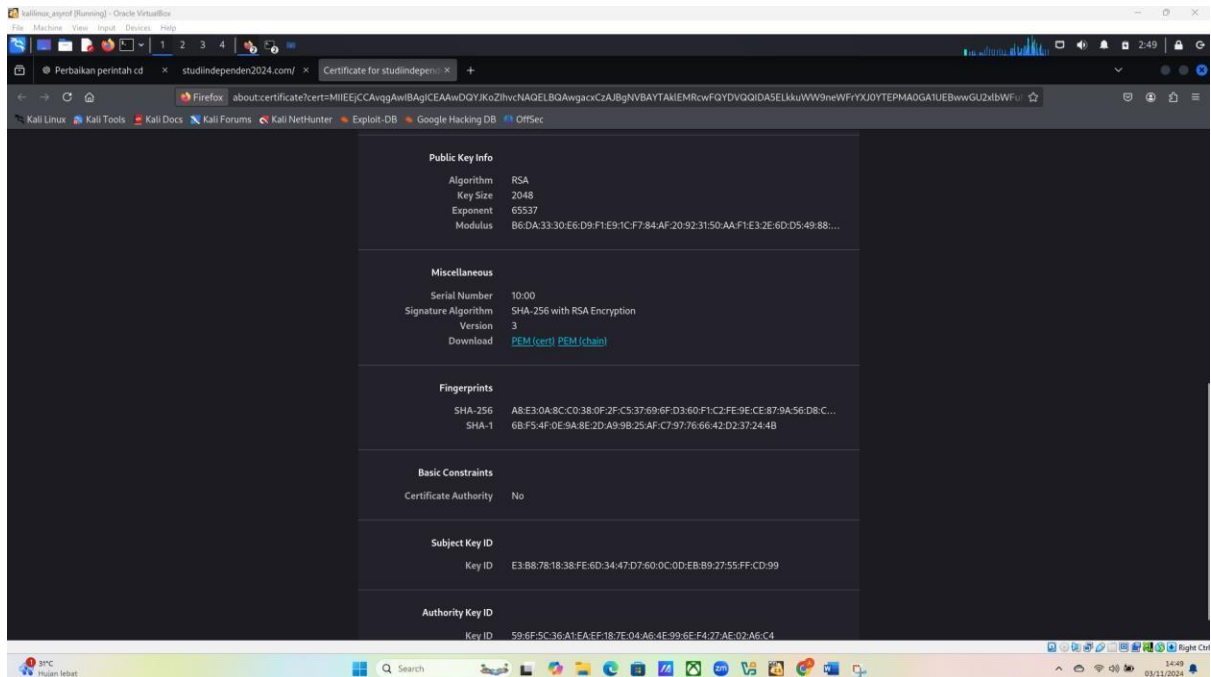
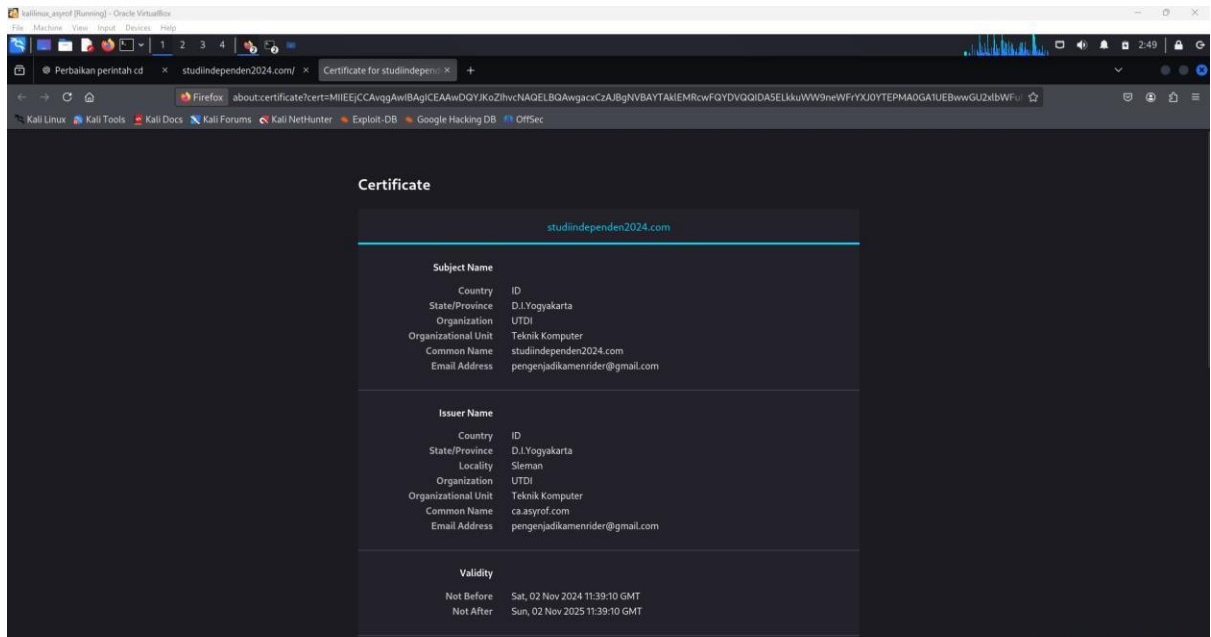
<https://studiindependen2024.com>



Selamat datang di studi independen 2024

Sertifikat studiindependen2024.com klik view certificate :





Buat yang sama untuk Asyrof-lab2024.com :

Pindah ke direktori konfigurasi apache dan buat file konfigurasi ssl untuk domain Asyrof-lab2024.com :





```
root@asyrof: /etc/apache2/sites-available

File Actions Edit View Help

<VirtualHost *:443>
    ServerAdmin webmaster@localhost studiindependen2024
    ServerName asyrof-lab2024.com
    DocumentRoot /var/www/asyrof-lab2024
    #<VirtualHost *:443>
    #   DocumentRoot /var/www/studiindependen2024

    SSLCertificateFile /etc/ssl/certs/asyrof-lab2024.com.crt
    SSLCertificateKeyFile /etc/ssl/private/asyrof-lab2024.com.key
```

Salin sertifikat ssl dan kunci private :

```
(root@asyrof)-[/home/asyrof/tugas]
# cp asyrof-lab2024.com.crt /etc/ssl/certs/
# cp asyrof-lab2024.com.key /etc/ssl/private/
# ls
asyrof-lab2024.com.crt  asyrof-lab2024.com.key  ca.key  openssl.cnf  studiindependen2024.com.csr
asyrof-lab2024.com.csr  ca.crt                  demoCA  studiindependen2024.com.crt  studiindependen2024.com.key
```

Mengaktifkan virtual host untuk ssl :

```
(root@asyrof)-[/home/asyrof/tugas]
# a2ensite asyrof-lab2024.com-ssl
Enabling site asyrof-lab2024.com-ssl.
To activate the new configuration, you need to run:
systemctl reload apache2
```

Reload apache2 untuk mengaktifkan konfigurasi baru :

```
(root@asyrof)-[/home/asyrof/tugas]
# systemctl reload apache2

Broadcast message from root@asyrof (Sun 2024-11-03 03:15:31 EST):

Password entry required for 'Enter passphrase for SSL/TLS keys for asyrof-lab2024.com:443 (RSA):' (PID 91816).
Please enter password with the systemd-tty-ask-password-agent tool.

(root@asyrof)-[/home/asyrof/tugas]
# systemctl reload apache2

Enter passphrase for SSL/TLS keys for asyrof-lab2024.com:443 (RSA): .....
```

Buat direktori web untuk domain :

```
(root@asyrof)-[/var/www]
# mkdir asyrof-lab2024
```

Buat file index.html sebagai halaman utama :

```
(root@asyrof)-[/home/asyrof/tugas]
# cd /var/www

(root@asyrof)-[/var/www]
# cd asyrof-lab2024

(root@asyrof)-[/var/www/asyrof-lab2024]
# ls

(root@asyrof)-[/var/www/asyrof-lab2024]
# vi index.html

(root@asyrof)-[/var/www/asyrof-lab2024]
# service apache2 reload

(root@asyrof)-[/var/www/asyrof-lab2024]
# ls
index.html
```

```
root@asyrof: /var/www/asyrof-lab2024

File Actions Edit View Help
Asyrof lab 2024!
|
```

Reload apache2 :

```
(root@asyrof)-[/etc/apache2/sites-available]
# systemctl reload apache2

(root@asyrof)-[/etc/apache2/sites-available]
#
Broadcast message from root@asyrof (Sun 2024-11-03 03:23:32 EST):

Password entry required for 'Enter passphrase for SSL/TLS keys for asyrof-lab2024.com:443 (RSA):' (PID 99738).
Please enter password with the systemd-tty-ask-password-agent tool.

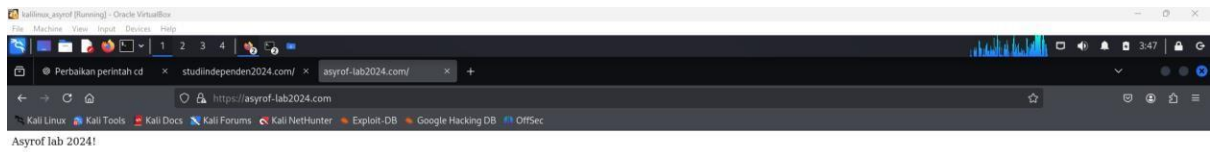
(root@asyrof)-[/etc/apache2/sites-available]
#

(root@asyrof)-[/etc/apache2/sites-available]
# systemctl reload apache2

🔒 Enter passphrase for SSL/TLS keys for asyrof-lab2024.com:443 (RSA): .....

(root@asyrof)-[/etc/apache2/sites-available]
#
```

Akses <https://asyrof-lab2024.com> :



Sertifikat Asyrof-lab2024.com klik view certificate :

