Workshop 6 – Transportation Layer Security

Task 1: Review Important Concepts

1. What services are provided by the TLS Record Protocol?

   Answer:

   Record layer protocol operations can be carried out after the initial TLS handshake process is successful. This is after the TLS handshake step has agreed to Key exchange, public key protocols, as well as the Cipher and key size to encrypt application data in the record layer and the hashing algorithm for the Message Authentication code.

   Thus, the negotiations between the end devices allow for message confidentiality and message integrity in the implementation of the record layer protocol.

   The record layer is where the exchange of application data happens after all the parameters are agreed on by both devices in the handshake protocol layer.

2. What steps are involved in the TLS Record Protocol transmission?

   Answer:
   In the record layer, encryption is performed on the application data followed by message authentication by the sender. This is the implementation that provides both integrity and confidentiality

   The receiving device decrypts and verifies the message using the Message Authentication Code (MAC) to ensure the data is not modified. This is similar to checksums to verify data integrity.

   Before the application data is transmitted it is fragmented (just like how data is fragmented into multiple packets in the IP protocol as an analogy), each fragmented segment can be compressed for faster transmission and less bandwidth on the network.

   Each Record layer fragment is appended with a MAC tag that contains a sequence number for reordering of fragments by the receiver to recover a meaningful representation of the application data.

   After this stage the tagged and optionally compressed fragment is encrypted, afterwards a header is prepended.

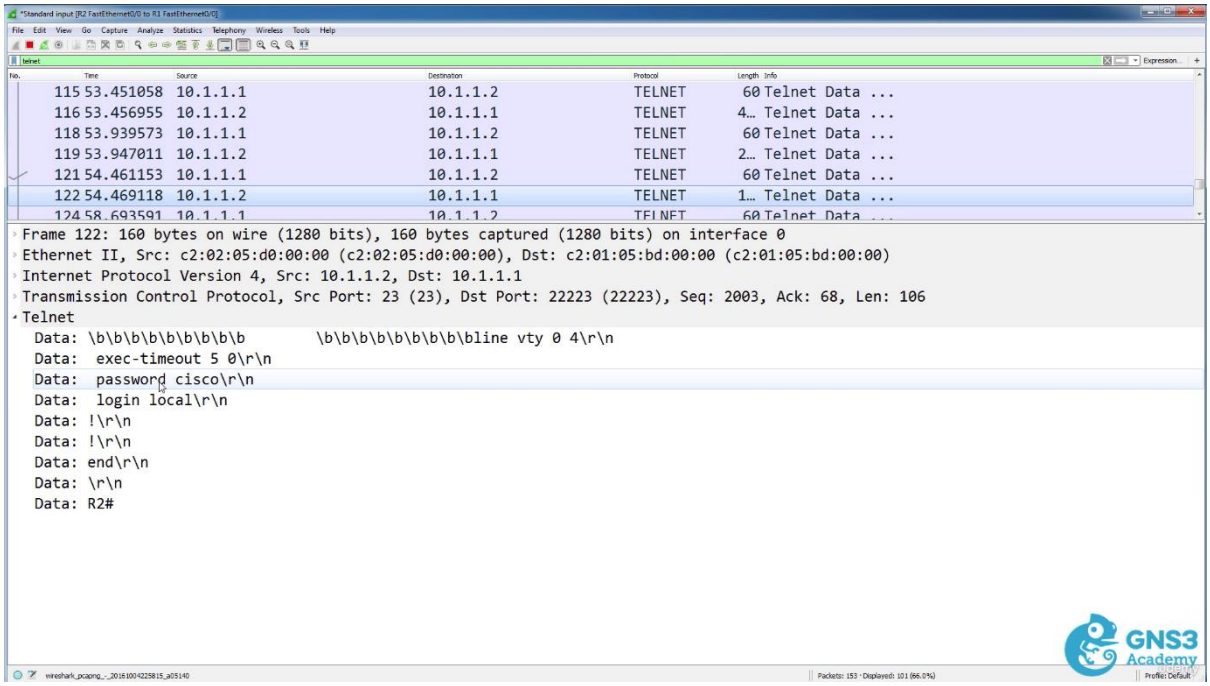
   The header is not encrypted like all headers in other layers in the packets and segments, otherwise the source and destination will not be clear for network devices between the end devices.

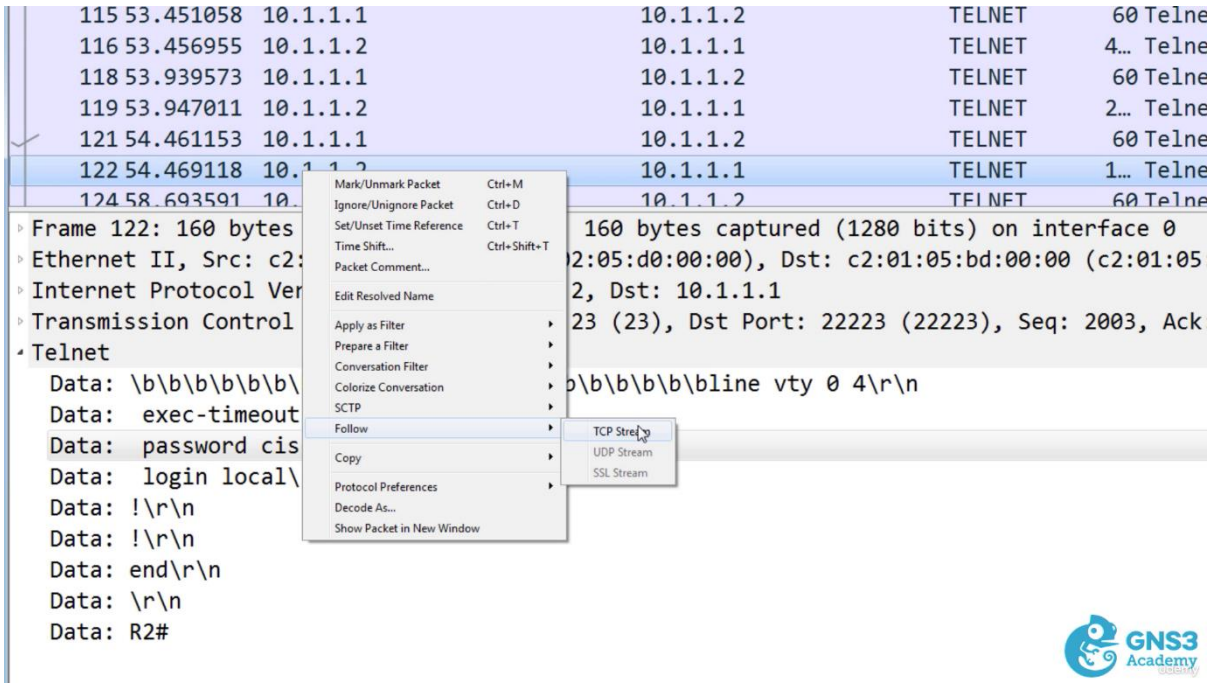
3. For what applications is SSH useful?

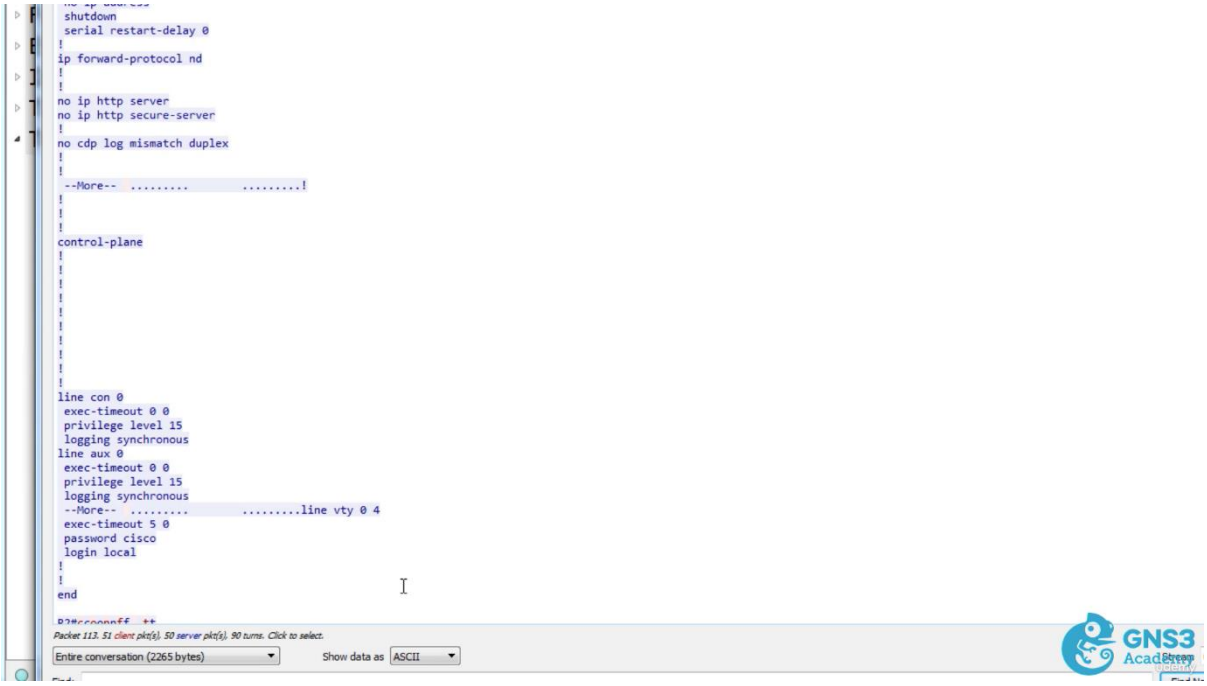
Answer:

Secure shell or SSH is used for secure remote access like telnet but it is more secure as the contents are encrypted.

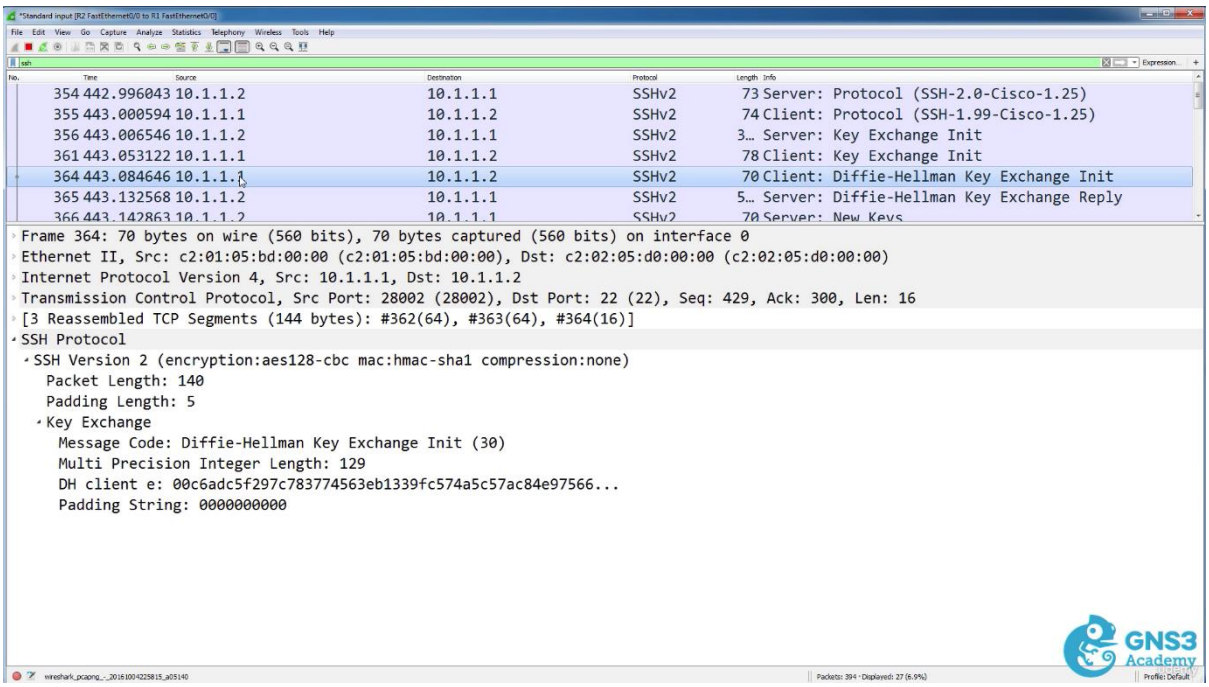
Below are examples of telnet traffic captured using Wireshark between two routers.

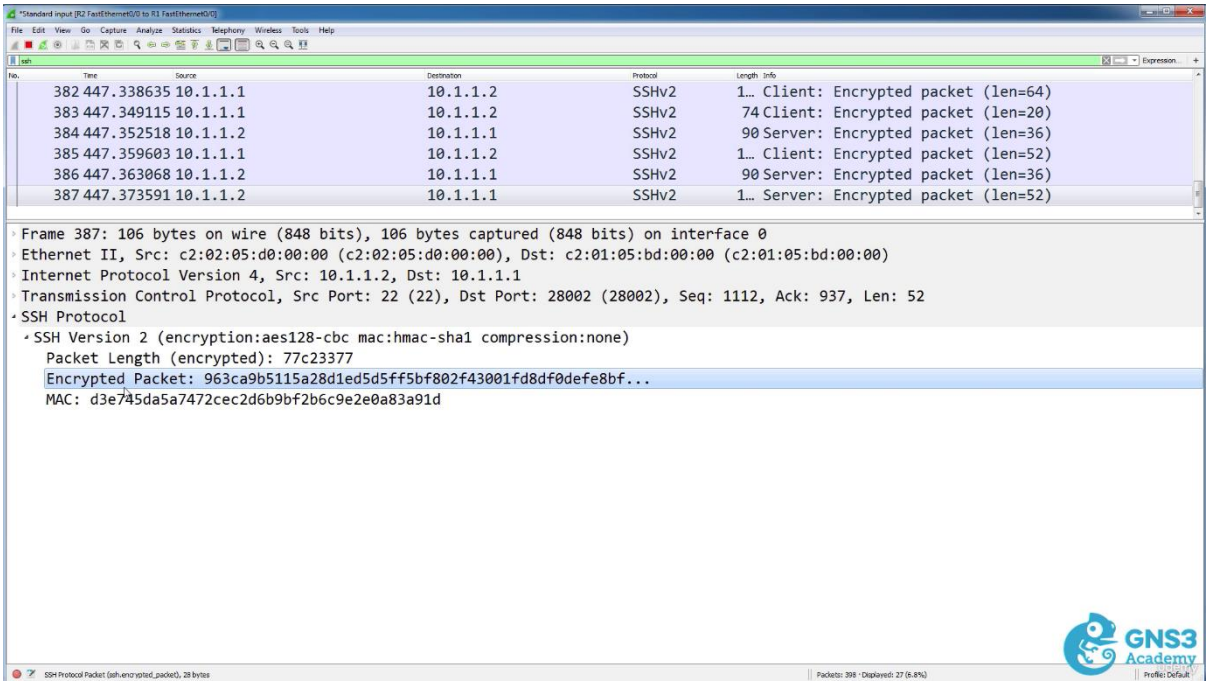






In the images below it shows SSH using Diffie-Hellman key exchange for encryption of transmitted data.



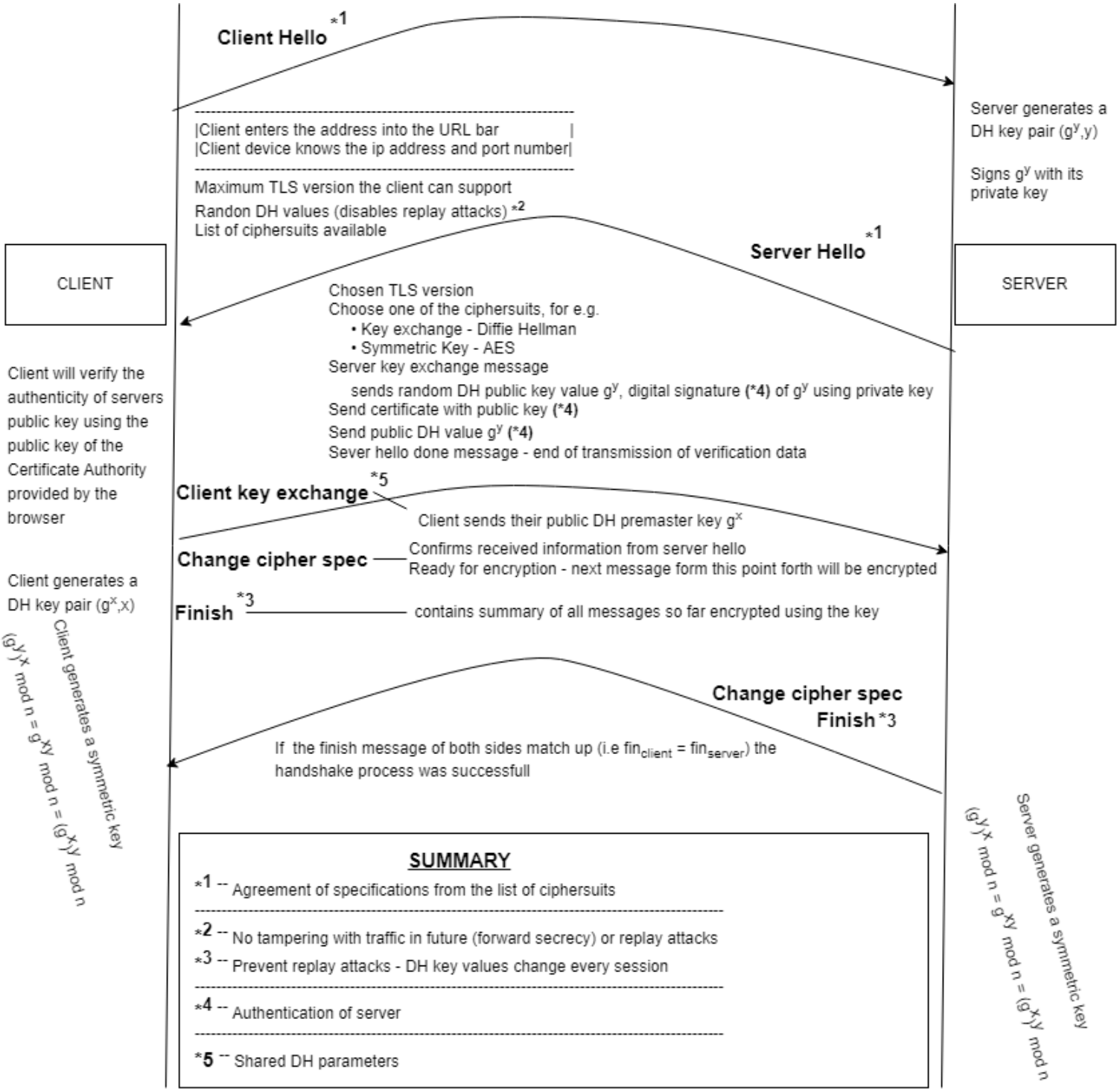


The second images show encrypted packets for confidentiality and a MAC tag value for data integrity. This is because SSH provides public key authentication of end devices and encryption.

For this reason, SSH is used for remote login, file transfer and limited VPN service. This protocol is also occasionally referred to as the “poor man’s VPN” (taken from the lecture 6 slide, 62, 2022)

4. Show the steps of TLS Handshake Protocol between a client and a server. Consider only server authentication and using Diffie-Hellman Key-Exchange Protocol for establishing shared secret keys. (It would be good to draw a diagram.)

   Answer:


Client Hello *1
Server generates a DH key pair (g^y,y)
Signs g^y with its private key
|Client enters the address into the URL bar |
|Client device knows the ip address and port number|
Maximum TLS version the client can support
Randon DH values (disables replay attacks) *2
List of ciphersuits available
Server Hello *1
CLIENT
SERVER
Chosen TLS version
Choose one of the ciphersuits, for e.g.
• Key exchange - Diffie Hellman
• Symmetric Key - AES
Server key exchange message
sends random DH public key value g^y, digital signature (*4) of g^y using private key
Send certificate with public key (*4)
Send public DH value g^y (*4)
Sever hello done message - end of transmission of verification data
Client will verify the authenticity of servers public key using the public key of the Certificate Authority provided by the browser
Client key exchange *5
Client sends their public DH premaster key g^x
Change cipher spec
Confirms received information from server hello
Ready for encryption - next message form this point forth will be encrypted
Client generates a DH key pair (g^x,x)
Finish *3
contains summary of all messages so far encrypted using the key
Client generates a symmetric key
(g^y)^x mod n = g^xy mod n = (g^x)^y mod n
Change cipher spec
Finish *3
If the finish message of both sides match up (i.e fin_client = fin_server) the handshake process was successfull
Server generates a symmetric key
(g^y)^x mod n = g^xy mod n = (g^x)^y mod n
SUMMARY
*1 -- Agreement of specifications from the list of ciphersuits
*2 -- No tampering with traffic in future (forward secrecy) or replay attacks
*3 -- Prevent replay attacks - DH key values change every session
*4 -- Authentication of server
*5 -- Shared DH parameters

Task 2: Establishing TLS Connections

This task is to demonstrate, how secure TLS connections are established. Please also answer questions in this task. This task is to be completed using Griffith Cyber Range.

Step 1. In this step, we will setup and generate CA's self-signed certificate. The public key in this certificate will be used by a client to verify web servers' certificates produced by that CA.

1. Copy the file openssl.cnf into the current directory

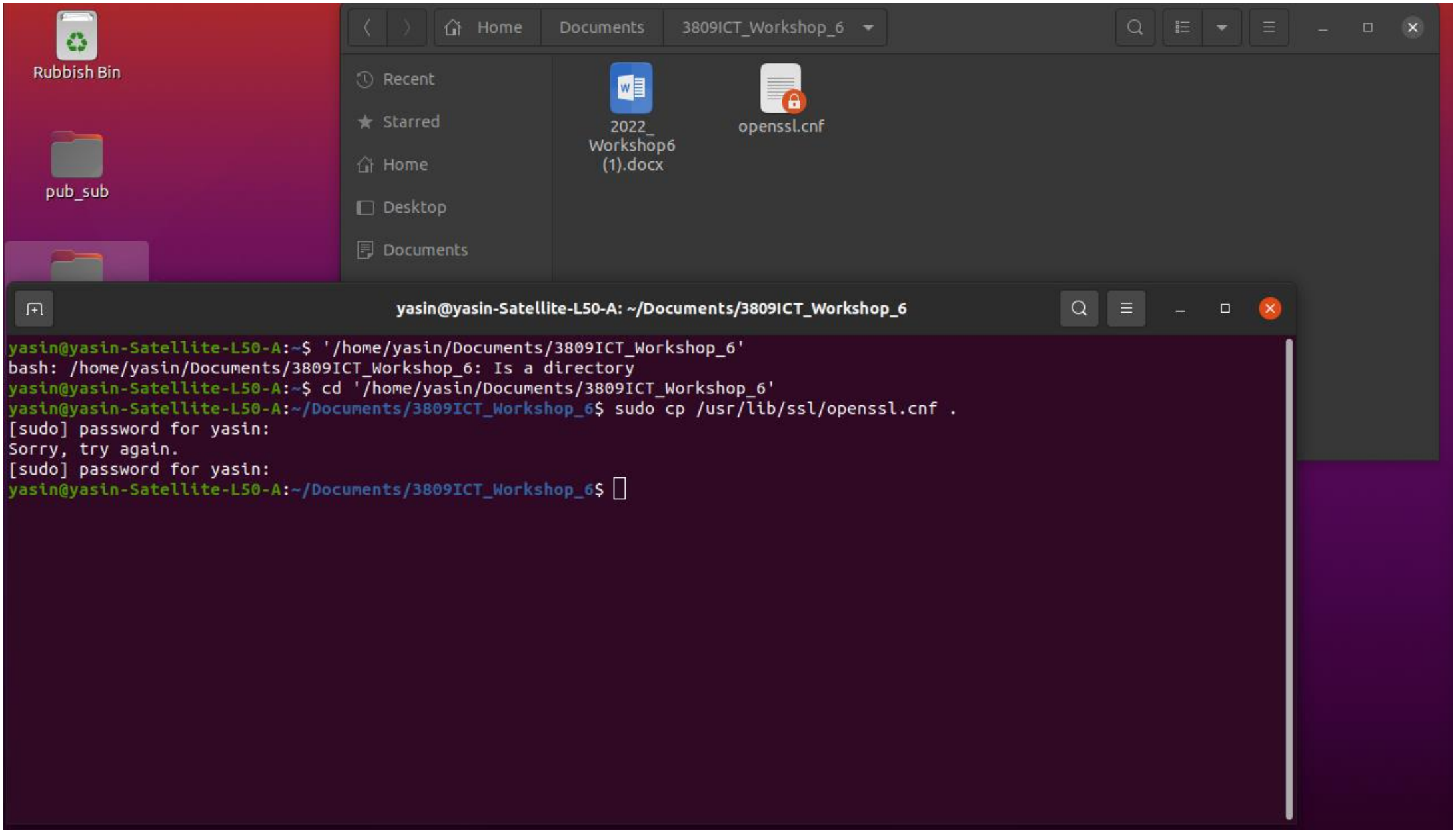
   ```
   $ sudo cp /usr/lib/ssl/openssl.cnf .
   # don't forget the dot.
   ```

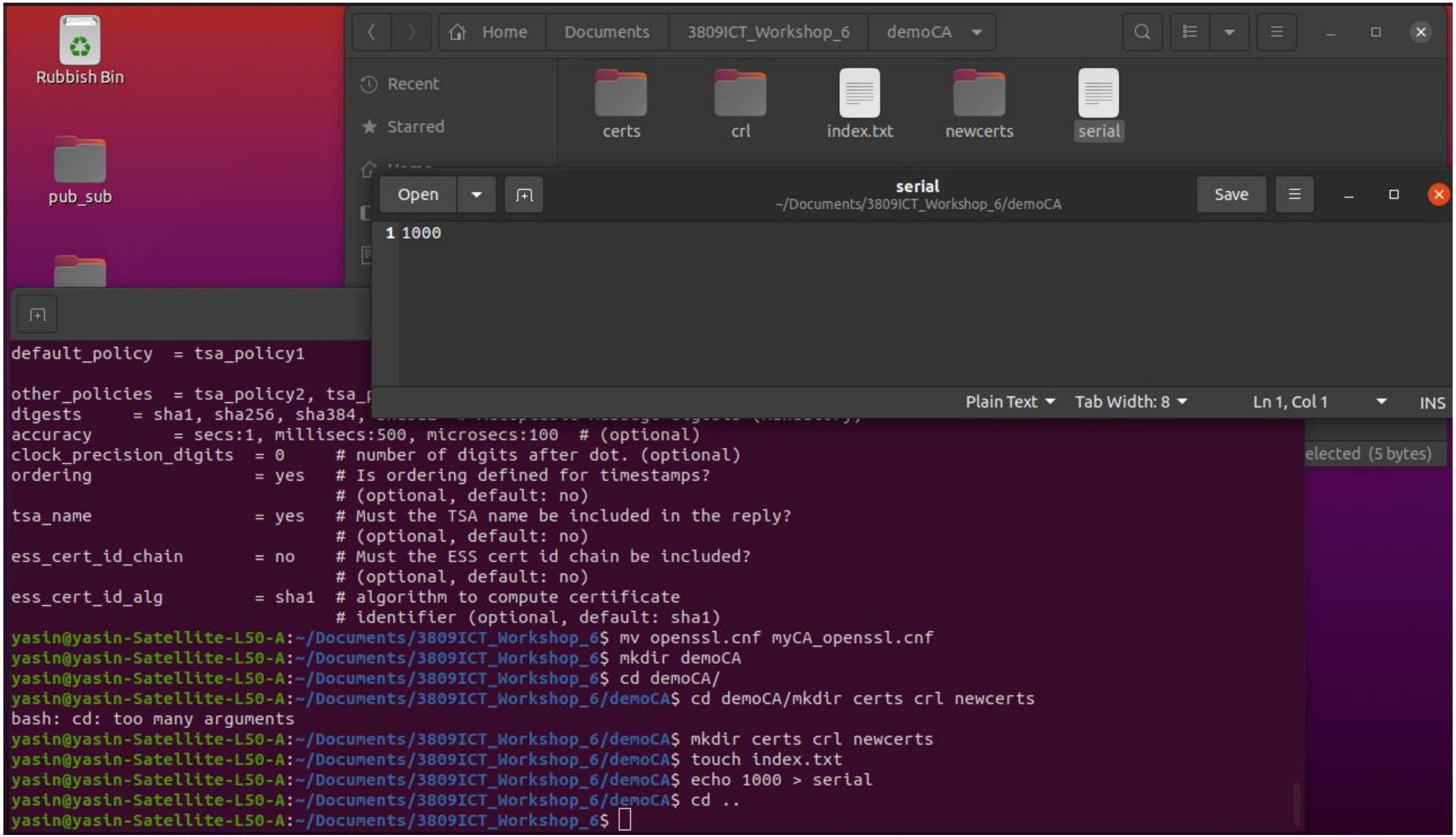
   Rename it as myCA_openssl.cnf. Create new directories.

   ```
   $ mkdir ./demoCA
   $ cd ./demoCA

   $ mkdir certs crl newcerts
   # create three directories under demoCA

   $ touch index.txt   # create an empty file index.txt
   $ echo 1000 > serial
   ```

   Go back to the directory /home/seed/ (e.g., by cd /home/seed).

   Answer:


Rubbish Bin
pub_sub
Home
Documents
3809ICT_Workshop_6
Recent
Starred
Home
Desktop
Documents
2022_ Workshop6 (1).docx
openssl.cnf
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
yasin@yasin-Satellite-L50-A:~$ '/home/yasin/Documents/3809ICT_Workshop_6'
bash: /home/yasin/Documents/3809ICT_Workshop_6: Is a directory
yasin@yasin-Satellite-L50-A:~$ cd '/home/yasin/Documents/3809ICT_Workshop_6'
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ sudo cp /usr/lib/ssl/openssl.cnf .
[sudo] password for yasin:
Sorry, try again.
[sudo] password for yasin:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$


Rubbish Bin
pub_sub
Home
Documents
3809ICT_Workshop_6
demoCA
Recent
Starred
certs
crl
index.txt
newcerts
serial
Open
serial
~/Documents/3809ICT_Workshop_6/demoCA
Save
1 1000
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
default_policy = tsa_policy1
other_policies = tsa_policy2, tsa_
digests = sha1, sha256, sha384,
accuracy = secs:1, millisecs:500, microsecs:100 # (optional)
clock_precision_digits = 0 # number of digits after dot. (optional)
ordering = yes # Is ordering defined for timestamps?
# (optional, default: no)
tsa_name = yes # Must the TSA name be included in the reply?
# (optional, default: no)
ess_cert_id_chain = no # Must the ESS cert id chain be included?
# (optional, default: no)
ess_cert_id_alg = sha1 # algorithm to compute certificate
# identifier (optional, default: sha1)
elected (5 bytes)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ mv openssl.cnf myCA_openssl.cnf
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ mkdir demoCA
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ cd demoCA/
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ cd demoCA/mkdir certs crl newcerts
bash: cd: too many arguments
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ mkdir certs crl newcerts
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ touch index.txt
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ echo 1000 > serial
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ cd ..
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$

2. Generate a self-signed digital certificate for CA.

```
$ openssl req -new -x509 -keyout ca.key -out ca.cert -config
myCA_openssl.cnf
```

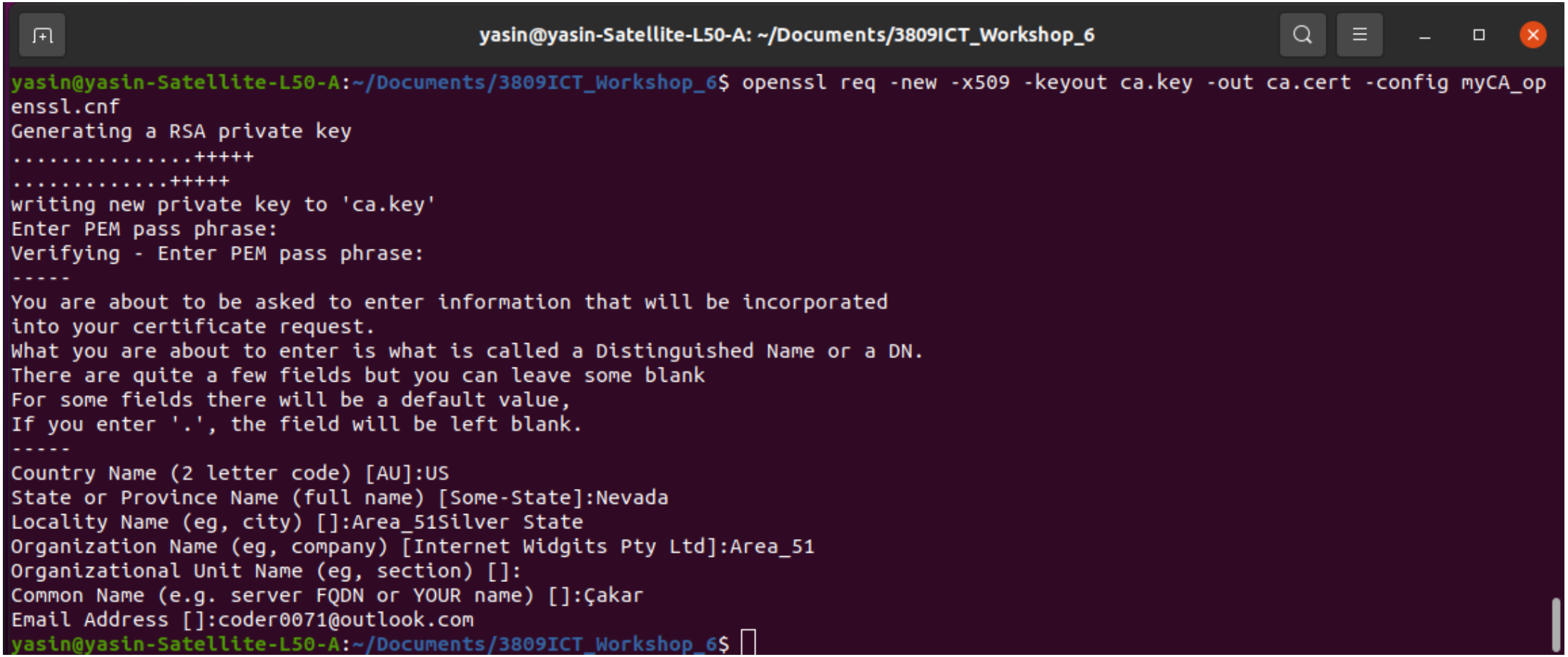
You will be asked for PEM phrase (a password used to protect the private key of CA). You will also be asked for other information. Looking ahead, since we will be using policy match between the server and the client, we fill out the following fields as below and the other fields with anything you want.

```
Country Name = AU
State Or Province Name = QLD
Organization Name = securitylab
```

To see the content of CA's certificate (i.e., ca.crt) and CA's private (signing) key (i.e., ca.key), you can issue the below commands. Please note the second one would ask for the PEM phrase.

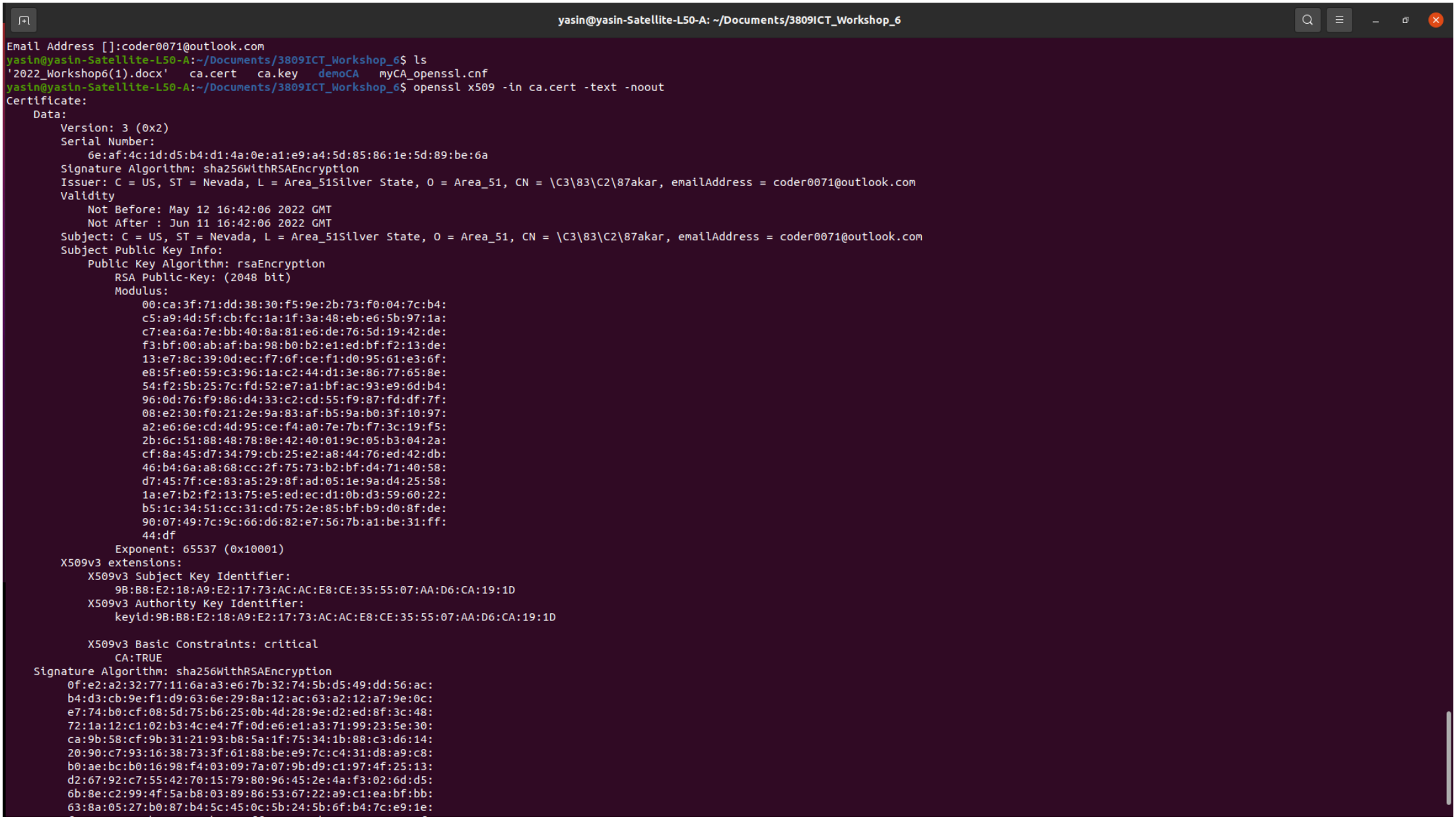
```
$ openssl x509 -in ca.cert -text -noout
$ openssl rsa -in ca.key -text -noout
```

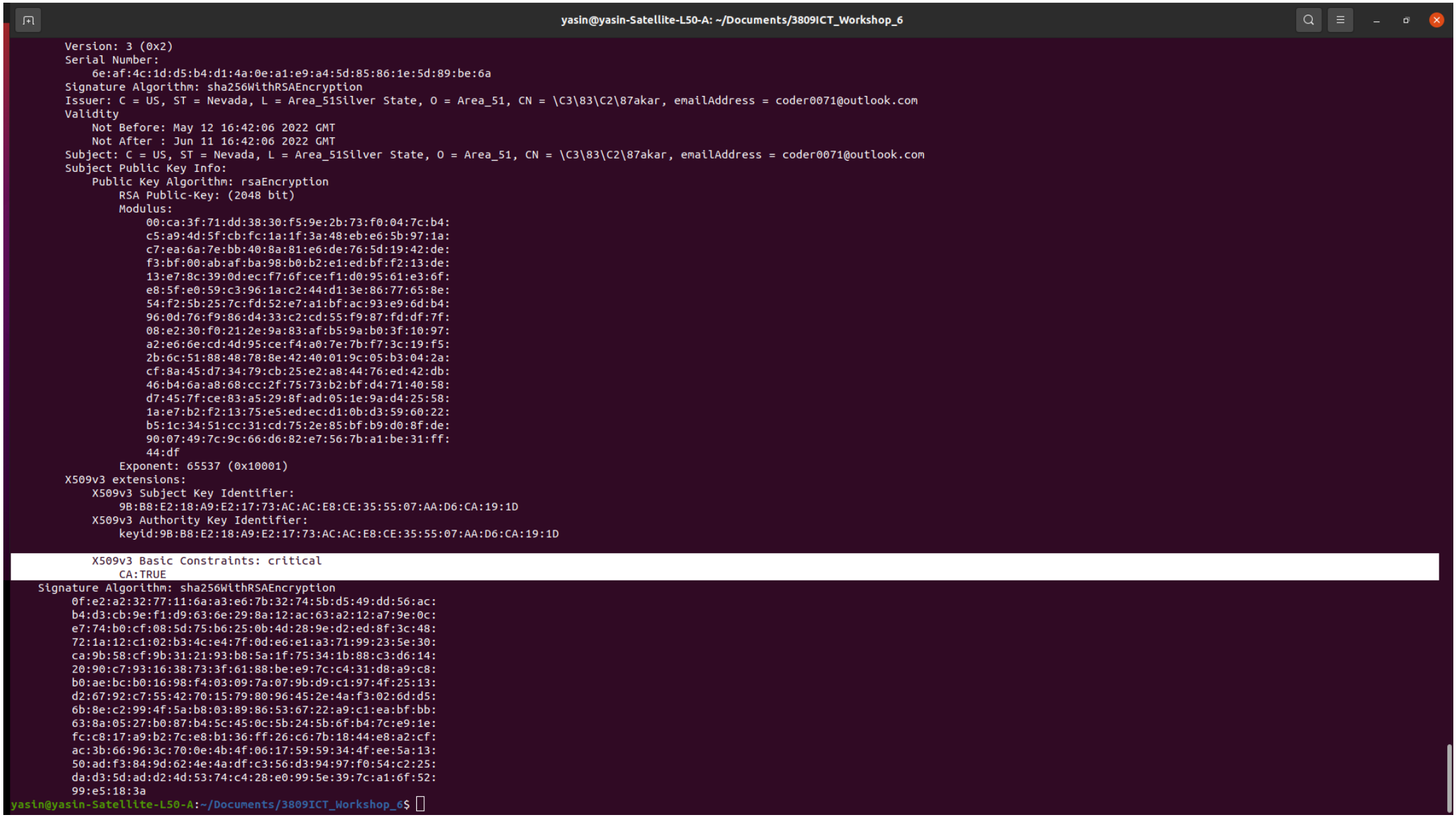
Answer:

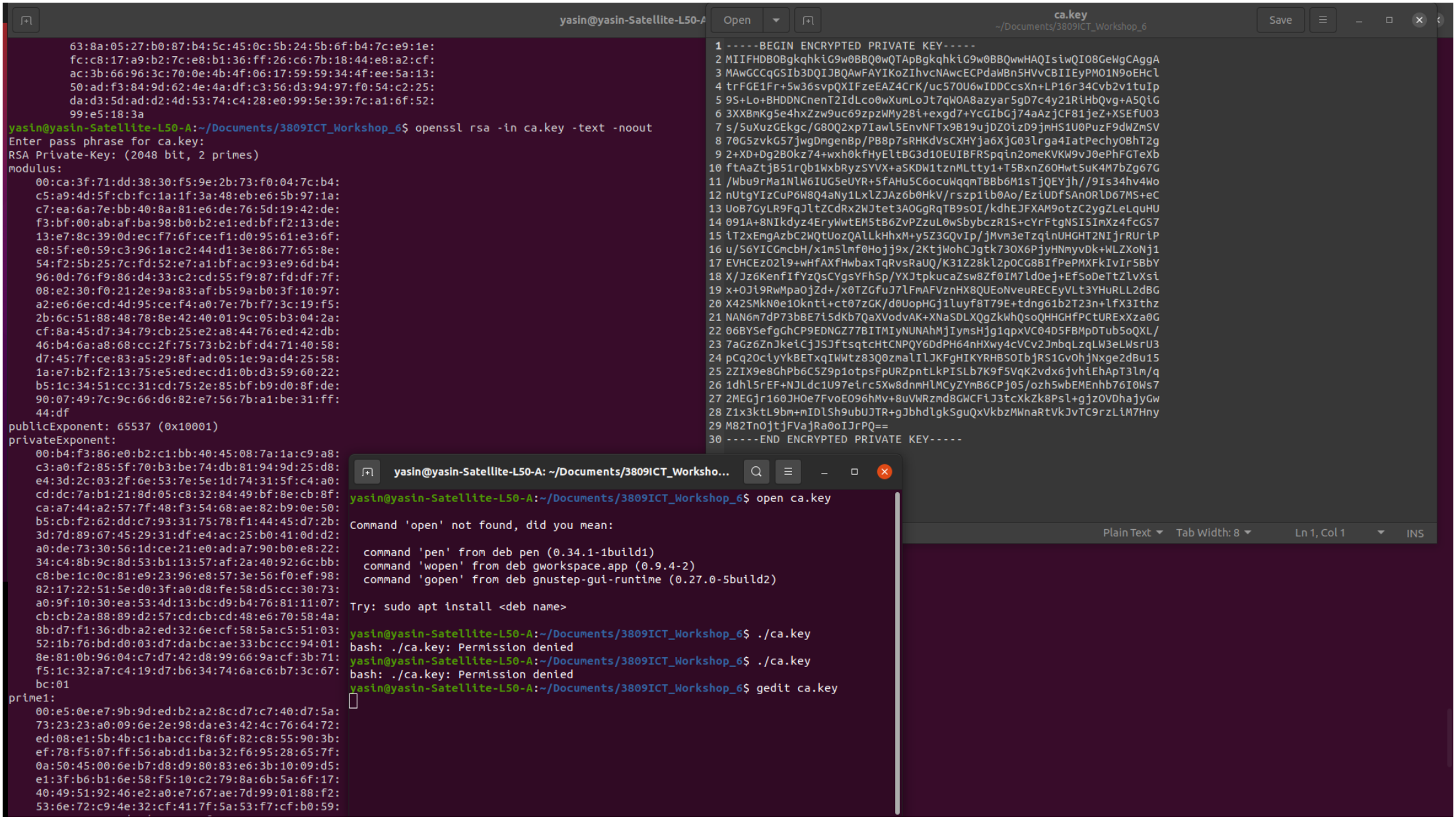

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl req -new -x509 -keyout ca.key -out ca.cert -config myCA_openssl.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

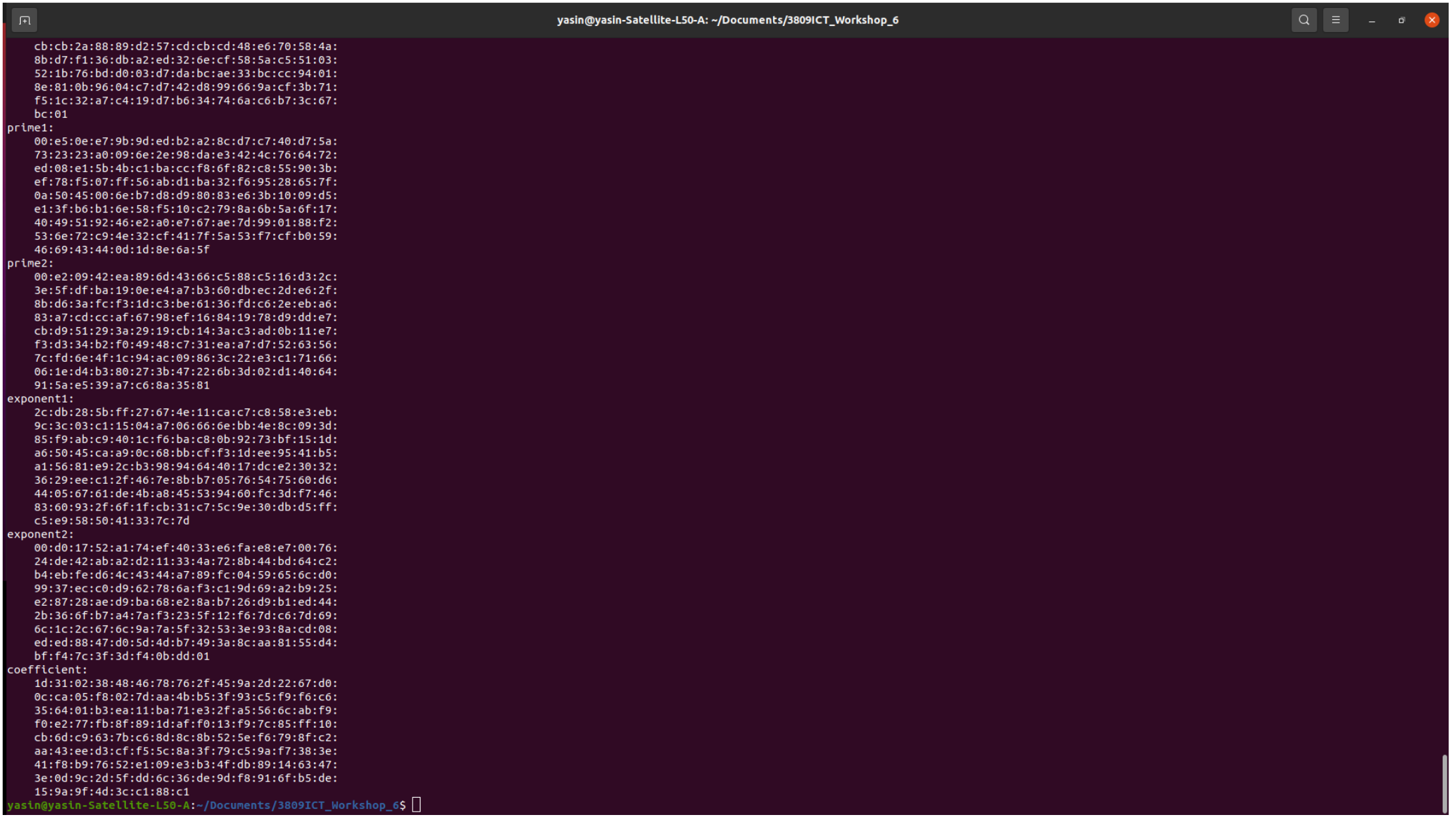
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Nevada
Locality Name (eg, city) []:Area_51Silver State
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Area_51
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Çakar
Email Address []:coder0071@outlook.com
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
Email Address []:coder0071@outlook.com
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ ls
'2022_Workshop6(1).docx' ca.cert ca.key demoCA myCA_openssl.cnf
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl x509 -in ca.cert -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
6e:af:4c:1d:d5:b4:d1:4a:0e:a1:e9:a4:5d:85:86:1e:5d:89:be:6a
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = Nevada, L = Area_51Silver State, O = Area_51, CN = \C3\83\C2\87akar, emailAddress = coder0071@outlook.com
Validity
Not Before: May 12 16:42:06 2022 GMT
Not After : Jun 11 16:42:06 2022 GMT
Subject: C = US, ST = Nevada, L = Area_51Silver State, O = Area_51, CN = \C3\83\C2\87akar, emailAddress = coder0071@outlook.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:ca:3f:71:dd:38:30:f5:9e:2b:73:f0:04:7c:b4:
c5:a9:4d:5f:cb:fc:1a:1f:3a:48:eb:e6:5b:97:1a:
c7:ea:6a:7e:bb:40:8a:81:e6:de:76:5d:19:42:de:
f3:bf:00:ab:af:ba:98:b0:b2:e1:ed:bf:f2:13:de:
13:e7:8c:39:0d:ec:f7:6f:ce:f1:d0:95:61:e3:6f:
e8:5f:e0:59:c3:96:1a:c2:44:d1:3e:86:77:65:8e:
54:f2:5b:25:7c:fd:52:e7:a1:bf:ac:93:e9:6d:b4:
96:0d:76:f9:86:d4:33:c2:cd:55:f9:87:fd:df:7f:
08:e2:30:f0:21:2e:9a:83:af:b5:9a:b0:3f:10:97:
a2:e6:6e:cd:4d:95:ce:f4:a0:7e:7b:f7:3c:19:f5:
2b:6c:51:88:48:78:8e:42:40:01:9c:05:b3:04:2a:
cf:8a:45:d7:34:79:cb:25:e2:a8:44:76:ed:42:db:
46:b4:6a:a8:68:cc:2f:75:73:b2:bf:d4:71:40:58:
d7:45:7f:ce:83:a5:29:8f:ad:05:1e:9a:d4:25:58:
1a:e7:b2:f2:13:75:e5:ed:ec:d1:0b:d3:59:60:22:
b5:1c:34:51:cc:31:cd:75:2e:85:bf:b9:d0:8f:de:
90:07:49:7c:9c:66:d6:82:e7:56:7b:a1:be:31:ff:
44:df
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
9B:B8:E2:18:A9:E2:17:73:AC:AC:E8:CE:35:55:07:AA:D6:CA:19:1D
X509v3 Authority Key Identifier:
keyid:9B:B8:E2:18:A9:E2:17:73:AC:AC:E8:CE:35:55:07:AA:D6:CA:19:1D
X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
0f:e2:a2:32:77:11:6a:a3:e6:7b:32:74:5b:d5:49:dd:56:ac:
b4:d3:cb:9e:f1:d9:63:6e:29:8a:12:ac:63:a2:12:a7:9e:0c:
e7:74:b0:cf:08:5d:75:b6:25:0b:4d:28:9e:d2:ed:8f:3c:48:
72:1a:12:c1:02:b3:4c:e4:7f:0d:e6:e1:a3:71:99:23:5e:30:
ca:9b:58:cf:9b:31:21:93:b8:5a:1f:75:34:1b:88:c3:d6:14:
20:90:c7:93:16:38:73:3f:61:88:be:e9:7c:c4:31:d8:a9:c8:
b0:ae:bc:b0:16:98:f4:03:09:7a:07:9b:d9:c1:97:4f:25:13:
d2:67:92:c7:55:42:70:15:79:80:96:45:2e:4a:f3:02:6d:d5:
6b:8e:c2:99:4f:5a:b8:03:89:86:53:67:22:a9:c1:ea:bf:bb:
63:8a:05:27:b0:87:b4:5c:45:0c:5b:24:5b:6f:b4:7c:e9:1e:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
Version: 3 (0x2)
Serial Number:
6e:af:4c:1d:d5:b4:d1:4a:0e:a1:e9:a4:5d:85:86:1e:5d:89:be:6a
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = Nevada, L = Area_51Silver State, O = Area_51, CN = \C3\83\C2\87akar, emailAddress = coder0071@outlook.com
Validity
Not Before: May 12 16:42:06 2022 GMT
Not After : Jun 11 16:42:06 2022 GMT
Subject: C = US, ST = Nevada, L = Area_51Silver State, O = Area_51, CN = \C3\83\C2\87akar, emailAddress = coder0071@outlook.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:ca:3f:71:dd:38:30:f5:9e:2b:73:f0:04:7c:b4:
c5:a9:4d:5f:cb:fc:1a:1f:3a:48:eb:e6:5b:97:1a:
c7:ea:6a:7e:bb:40:8a:81:e6:de:76:5d:19:42:de:
f3:bf:00:ab:af:ba:98:b0:b2:e1:ed:bf:f2:13:de:
13:e7:8c:39:0d:ec:f7:6f:ce:f1:d0:95:61:e3:6f:
e8:5f:e0:59:c3:96:1a:c2:44:d1:3e:86:77:65:8e:
54:f2:5b:25:7c:fd:52:e7:a1:bf:ac:93:e9:6d:b4:
96:0d:76:f9:86:d4:33:c2:cd:55:f9:87:fd:df:7f:
08:e2:30:f0:21:2e:9a:83:af:b5:9a:b0:3f:10:97:
a2:e6:6e:cd:4d:95:ce:f4:a0:7e:7b:f7:3c:19:f5:
2b:6c:51:88:48:78:8e:42:40:01:9c:05:b3:04:2a:
cf:8a:45:d7:34:79:cb:25:e2:a8:44:76:ed:42:db:
46:b4:6a:a8:68:cc:2f:75:73:b2:bf:d4:71:40:58:
d7:45:7f:ce:83:a5:29:8f:ad:05:1e:9a:d4:25:58:
1a:e7:b2:f2:13:75:e5:ed:ec:d1:0b:d3:59:60:22:
b5:1c:34:51:cc:31:cd:75:2e:85:bf:b9:d0:8f:de:
90:07:49:7c:9c:66:d6:82:e7:56:7b:a1:be:31:ff:
44:df
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
9B:B8:E2:18:A9:E2:17:73:AC:AC:E8:CE:35:55:07:AA:D6:CA:19:1D
X509v3 Authority Key Identifier:
keyid:9B:B8:E2:18:A9:E2:17:73:AC:AC:E8:CE:35:55:07:AA:D6:CA:19:1D
X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
0f:e2:a2:32:77:11:6a:a3:e6:7b:32:74:5b:d5:49:dd:56:ac:
b4:d3:cb:9e:f1:d9:63:6e:29:8a:12:ac:63:a2:12:a7:9e:0c:
e7:74:b0:cf:08:5d:75:b6:25:0b:4d:28:9e:d2:ed:8f:3c:48:
72:1a:12:c1:02:b3:4c:e4:7f:0d:e6:e1:a3:71:99:23:5e:30:
ca:9b:58:cf:9b:31:21:93:b8:5a:1f:75:34:1b:88:c3:d6:14:
20:90:c7:93:16:38:73:3f:61:88:be:e9:7c:c4:31:d8:a9:c8:
b0:ae:bc:b0:16:98:f4:03:09:7a:07:9b:d9:c1:97:4f:25:13:
d2:67:92:c7:55:42:70:15:79:80:96:45:2e:4a:f3:02:6d:d5:
6b:8e:c2:99:4f:5a:b8:03:89:86:53:67:22:a9:c1:ea:bf:bb:
63:8a:05:27:b0:87:b4:5c:45:0c:5b:24:5b:6f:b4:7c:e9:1e:
fc:c8:17:a9:b2:7c:e8:b1:36:ff:26:c6:7b:18:44:e8:a2:cf:
ac:3b:66:96:3c:70:0e:4b:4f:06:17:59:59:34:4f:ee:5a:13:
50:ad:f3:84:9d:62:4e:4a:df:c3:56:d3:94:97:f0:54:c2:25:
da:d3:5d:ad:d2:4d:53:74:c4:28:e0:99:5e:39:7c:a1:6f:52:
99:e5:18:3a
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$


yasin@yasin-Satellite-L50-A
63:8a:05:27:b0:87:b4:5c:45:0c:5b:24:5b:6f:b4:7c:e9:1e:
fc:c8:17:a9:b2:7c:e8:b1:36:ff:26:c6:7b:18:44:e8:a2:cf:
ac:3b:66:96:3c:70:0e:4b:4f:06:17:59:59:34:4f:ee:5a:13:
50:ad:f3:84:9d:62:4e:4a:df:c3:56:d3:94:97:f0:54:c2:25:
da:d3:5d:ad:d2:4d:53:74:c4:28:e0:99:5e:39:7c:a1:6f:52:
99:e5:18:3a
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl rsa -in ca.key -text -noout
Enter pass phrase for ca.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
00:ca:3f:71:dd:38:30:f5:9e:2b:73:f0:04:7c:b4:
c5:a9:4d:5f:cb:fc:1a:1f:3a:48:eb:e6:5b:97:1a:
c7:ea:6a:7e:bb:40:8a:81:e6:de:76:5d:19:42:de:
f3:bf:00:ab:af:ba:98:b0:b2:e1:ed:bf:f2:13:de:
13:e7:8c:39:0d:ec:f7:6f:ce:f1:d0:95:61:e3:6f:
e8:5f:e0:59:c3:96:1a:c2:44:d1:3e:86:77:65:8e:
54:f2:5b:25:7c:fd:52:e7:a1:bf:ac:93:e9:6d:b4:
96:0d:76:f9:86:d4:33:c2:cd:55:f9:87:fd:df:7f:
08:e2:30:f0:21:2e:9a:83:af:b5:9a:b0:3f:10:97:
a2:e6:6e:cd:4d:95:ce:f4:a0:7e:7b:f7:3c:19:f5:
2b:6c:51:88:48:78:8e:42:40:01:9c:05:b3:04:2a:
cf:8a:45:d7:34:79:cb:25:e2:a8:44:76:ed:42:db:
46:b4:6a:a8:68:cc:2f:75:73:b2:bf:d4:71:40:58:
d7:45:7f:ce:83:a5:29:8f:ad:05:1e:9a:d4:25:58:
1a:e7:b2:f2:13:75:e5:ed:ec:d1:0b:d3:59:60:22:
b5:1c:34:51:cc:31:cd:75:2e:85:bf:b9:d0:8f:de:
90:07:49:7c:9c:66:d6:82:e7:56:7b:a1:be:31:ff:
44:df
publicExponent: 65537 (0x10001)
privateExponent:
00:b4:f3:86:e0:b2:c1:bb:40:45:08:7a:1a:c9:a8:
c3:a0:f2:85:5f:70:b3:be:74:db:81:94:9d:25:d8:
e4:3d:2c:03:2f:6e:53:7e:5e:1d:74:31:5f:c4:a0:
cd:dc:7a:b1:21:8d:05:c8:32:84:49:bf:8e:cb:8f:
ca:a7:44:a2:57:7f:48:f3:54:68:ae:82:b9:0e:50:
b5:cb:f2:62:dd:c7:93:31:75:78:f1:44:45:d7:2b:
3d:7d:89:67:45:29:31:df:e4:ac:25:b0:41:0d:d2:
a0:de:73:30:56:1d:ce:21:e0:ad:a7:90:b0:e8:22:
34:c4:8b:9c:8d:53:b1:13:57:af:2a:40:92:6c:bb:
c8:be:1c:0c:81:e9:23:96:e8:57:3e:56:f0:ef:98:
82:17:22:51:5e:d0:3f:a0:d8:fe:58:d5:cc:30:73:
a0:9f:10:30:ea:53:4d:13:bc:d9:b4:76:81:11:07:
cb:cb:2a:88:89:d2:57:cd:cb:cd:48:e6:70:58:4a:
8b:d7:f1:36:db:a2:ed:32:6e:cf:58:5a:c5:51:03:
52:1b:76:bd:d0:03:d7:da:bc:ae:33:bc:cc:94:01:
8e:81:0b:96:04:c7:d7:42:d8:99:66:9a:cf:3b:71:
f5:1c:32:a7:c4:19:d7:b6:34:74:6a:c6:b7:3c:67:
bc:01
prime1:
00:e5:0e:e7:9b:9d:ed:b2:a2:8c:d7:c7:40:d7:5a:
73:23:23:a0:09:6e:2e:98:da:e3:42:4c:76:64:72:
ed:08:e1:5b:4b:c1:ba:cc:f8:6f:82:c8:55:90:3b:
ef:78:f5:07:ff:56:ab:d1:ba:32:f6:95:28:65:7f:
0a:50:45:00:6e:b7:d8:d9:80:83:e6:3b:10:09:d5:
e1:3f:b6:b1:6e:58:f5:10:c2:79:8a:6b:5a:6f:17:
40:49:51:92:46:e2:a0:e7:67:ae:7d:99:01:88:f2:
53:6e:72:c9:4e:32:cf:41:7f:5a:53:f7:cf:b0:59:
Open
ca.key
~/Documents/3809ICT_Workshop_6
Save
1 -----BEGIN ENCRYPTED PRIVATE KEY-----
2 MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIsiwQIO8GeWgCAggA
3 MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECPdaWBn5HVvCBIIEyPMO1N9oEHcl
4 trFGE1Fr+5w36svpQXIFzeEAZ4CrK/uc57OU6wIDDCcsXn+LP16r34Cvb2v1tuIp
5 9S+Lo+BHDDNCnenT2IdLco0wXumLoJt7qWOA8azyar5gD7c4y21RiHbQvg+A5QiG
6 3XXBmKg5e4hxZzw9uc69zpzWMy28i+exgd7+YcGIbGj74aAzjCF81jeZ+XSEfUO3
7 s/5uXuzGEkgc/G8OQ2xp7Iawl5EnvNFTx9B19ujDZOizD9jmHS1U0PuzF9dWZmSV
8 70G5zvkG57jwgDmgenBp/PB8p7sRHKdVsCXHYja6XjG03lrga4IatPechyOBhT2g
9 2+XD+Dg2BOkz74+wxh0kfHyEltBG3d1OEUIBFRSpqin2omeKVKW9vJ0ePhFGTeXb
10 ftAaZtjB51rQb1WxbRyzSYVX+aSKDW1tznMLtty1+T5BxnZ6OHwt5uK4M7bZg67G
11 /Wbu9rMa1NlW6IUG5eUYR+5fAHu5C6ocuWqqmTBBb6M1sTjQEYjh//9Is34hv4Wo
12 nUtgYIzCuP6W8Q4aNy1LxlZJAz6b0HkV/rszp1ib0Ao/EziUDfSAnORlD67MS+eC
13 UoB7GyLR9FqJltZCdRx2WJtet3AOGgRqTB9sOI/kdhEJFXAM9otzC2ygZLeLquHU
14 091A+8NIkdyz4EryWwtEM5tB6ZvPZzuL0wSbybczR1S+cYrFtgNSI5ImXz4fcGS7
15 iT2xEmgAzbC2WQtUozQAlLkHhxM+y5Z3GQvIp/jMvm3eTzqinUHGHT2NIjrRUriP
16 u/S6YICGmcbH/x1m5lmf0Hojj9x/2KtjWohCJgtk73OX6PjyHNmyvDk+WLZXoNj1
17 EVHCEzO2l9+wHfAXfHwbaxTqRvsRaUQ/K31Z28kl2pOCG8BIfPePMXFkIvIr5BbY
18 X/Jz6KenfIfYzQsCYgsYFhSp/YXJtpkucaZsw8Zf0IM7ldOej+EfSoDeTtZlvXsi
19 x+OJi9RwMpaOjZd+/x0TZGfuJ7lFmAFVznHX8QUEoNveuRECEyVLt3YHuRLL2dBG
20 X42SMkN0e1Oknti+ct07zGK/d0UopHGj1luyf8T79E+tdng61b2T23n+lfX3Ithz
21 NAN6m7dP73bBE7i5dKb7QaXVodvAK+XNaSDLXQgZkWhQsoQHHGHfPCtURExXza0G
22 06BYSefgGhCP9EDNGZ77BITMIyNUNAhMjIymsHjg1qpxVC04D5FBMpDTub5oQXL/
23 7aGz6ZnJkeiCjJSJftsqtcHtCNPQY6DdPH64nHXwy4cVCv2JmbqLzqLW3eLWsrU3
24 pCq2OciyYkBETxqIWWtz83Q0zmalIlJKFgHIKYRHBSOIbjRS1GvOhjNxge2dBu15
25 2ZIX9e8GhPb6C5Z9p1otpsFpURZpntLkPISLb7K9f5VqK2vdx6jvhiEhApT3lm/q
26 1dhl5rEF+NJLdc1U97eirc5Xw8dnmHlMCyZYmB6CPj05/ozh5wbEMEnhb76I0Ws7
27 2MEGjr160JHOe7FvoEO96hMv+8uVWRzmd8GWCFiJ3tcXkZk8Psl+gjzOVDhajyGw
28 Z1x3ktL9bm+mIDlSh9ubUJTR+gJbhdlgkSguQxVkbzMWnaRtVkJvTC9rzLiM7Hny
29 M82TnOjtjFVajRa0oIJrPQ==
30 -----END ENCRYPTED PRIVATE KEY-----
Plain Text
Tab Width: 8
Ln 1, Col 1
INS
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Worksho...
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ open ca.key
Command 'open' not found, did you mean:
command 'pen' from deb pen (0.34.1-1build1)
command 'wopen' from deb gworkspace.app (0.9.4-2)
command 'gopen' from deb gnustep-gui-runtime (0.27.0-5build2)
Try: sudo apt install <deb name>
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ ./ca.key
bash: ./ca.key: Permission denied
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ ./ca.key
bash: ./ca.key: Permission denied
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ gedit ca.key

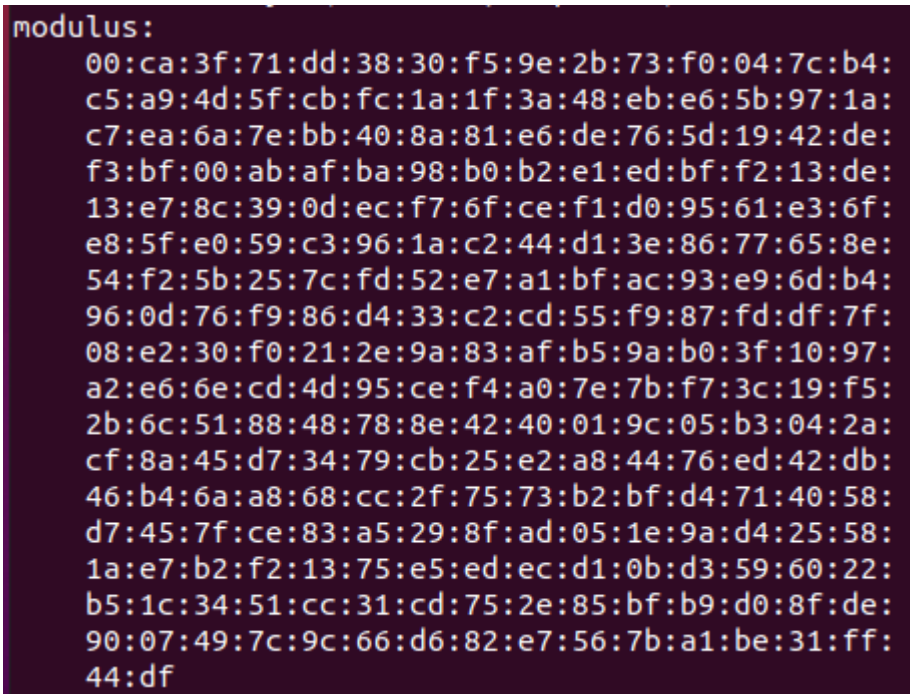

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
cb:cb:2a:88:89:d2:57:cd:cb:cd:48:e6:70:58:4a:
8b:d7:f1:36:db:a2:ed:32:6e:cf:58:5a:c5:51:03:
52:1b:76:bd:d0:03:d7:da:bc:ae:33:bc:cc:94:01:
8e:81:0b:96:04:c7:d7:42:d8:99:66:9a:cf:3b:71:
f5:1c:32:a7:c4:19:d7:b6:34:74:6a:c6:b7:3c:67:
bc:01
prime1:
00:e5:0e:e7:9b:9d:ed:b2:a2:8c:d7:c7:40:d7:5a:
73:23:23:a0:09:6e:2e:98:da:e3:42:4c:76:64:72:
ed:08:e1:5b:4b:c1:ba:cc:f8:6f:82:c8:55:90:3b:
ef:78:f5:07:ff:56:ab:d1:ba:32:f6:95:28:65:7f:
0a:50:45:00:6e:b7:d8:d9:80:83:e6:3b:10:09:d5:
e1:3f:b6:b1:6e:58:f5:10:c2:79:8a:6b:5a:6f:17:
40:49:51:92:46:e2:a0:e7:67:ae:7d:99:01:88:f2:
53:6e:72:c9:4e:32:cf:41:7f:5a:53:f7:cf:b0:59:
46:69:43:44:0d:1d:8e:6a:5f
prime2:
00:e2:09:42:ea:89:6d:43:66:c5:88:c5:16:d3:2c:
3e:5f:df:ba:19:0e:e4:a7:b3:60:db:ec:2d:e6:2f:
8b:d6:3a:fc:f3:1d:c3:be:61:36:fd:c6:2e:eb:a6:
83:a7:cd:cc:af:67:98:ef:16:84:19:78:d9:dd:e7:
cb:d9:51:29:3a:29:19:cb:14:3a:c3:ad:0b:11:e7:
f3:d3:34:b2:f0:49:48:c7:31:ea:a7:d7:52:63:56:
7c:fd:6e:4f:1c:94:ac:09:86:3c:22:e3:c1:71:66:
06:1e:d4:b3:80:27:3b:47:22:6b:3d:02:d1:40:64:
91:5a:e5:39:a7:c6:8a:35:81
exponent1:
2c:db:28:5b:ff:27:67:4e:11:ca:c7:c8:58:e3:eb:
9c:3c:03:c1:15:04:a7:06:66:6e:bb:4e:8c:09:3d:
85:f9:ab:c9:40:1c:f6:ba:c8:0b:92:73:bf:15:1d:
a6:50:45:ca:a9:0c:68:bb:cf:f3:1d:ee:95:41:b5:
a1:56:81:e9:2c:b3:98:94:64:40:17:dc:e2:30:32:
36:29:ee:c1:2f:46:7e:8b:b7:05:76:54:75:60:d6:
44:05:67:61:de:4b:a8:45:53:94:60:fc:3d:f7:46:
83:60:93:2f:6f:1f:cb:31:c7:5c:9e:30:db:d5:ff:
c5:e9:58:50:41:33:7c:7d
exponent2:
00:d0:17:52:a1:74:ef:40:33:e6:fa:e8:e7:00:76:
24:de:42:ab:a2:d2:11:33:4a:72:8b:44:bd:64:c2:
b4:eb:fe:d6:4c:43:44:a7:89:fc:04:59:65:6c:d0:
99:37:ec:c0:d9:62:78:6a:f3:c1:9d:69:a2:b9:25:
e2:87:28:ae:d9:ba:68:e2:8a:b7:26:d9:b1:ed:44:
2b:36:6f:b7:a4:7a:f3:23:5f:12:f6:7d:c6:7d:69:
6c:1c:2c:67:6c:9a:7a:5f:32:53:3e:93:8a:cd:08:
ed:ed:88:47:d0:5d:4d:b7:49:3a:8c:aa:81:55:d4:
bf:f4:7c:3f:3d:f4:0b:dd:01
coefficient:
1d:31:02:38:48:46:78:76:2f:45:9a:2d:22:67:d0:
0c:ca:05:f8:02:7d:aa:4b:b5:3f:93:c5:f9:f6:c6:
35:64:01:b3:ea:11:ba:71:e3:2f:a5:56:6c:ab:f9:
f0:e2:77:fb:8f:89:1d:af:f0:13:f9:7c:85:ff:10:
cb:6d:c9:63:7b:c6:8d:8c:8b:52:5e:f6:79:8f:c2:
aa:43:ee:d3:cf:f5:5c:8a:3f:79:c5:9a:f7:38:3e:
41:f8:b9:76:52:e1:09:e3:b3:4f:db:89:14:63:47:
3e:0d:9c:2d:5f:dd:6c:36:de:9d:f8:91:6f:b5:de:
15:9a:9f:4d:3c:c1:88:c1
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$

Q: What part of the certificate indicates this is a CA's certificate?
Answer:
The issuer and subject details are the same (see the 3rd or 4th image)

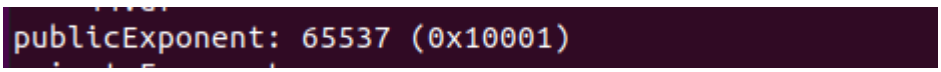
Q: What part of the certificate indicates this is a self-signed certificate?
Answer:
Inside the Certificate Authoritie's certificate theresi a line tha shows the certificate was signed using the private key of the certificate authority itself:

“”“
X5093 Basic Constraints: critical
CA:TRUE
“”“

Q: In the RSA algorithm, we have a public exponent *e*, a private exponent *d*, a modulus *n*, and two secret numbers *p* and *q*, such that $n = pq$. Please identify the values for these elements in your certificate and key files.
Answer:
Modulus, n:



Exponent, e:



Prime numbers, p & q:

```
prime1:
    00:e5:0e:e7:9b:9d:ed:b2:a2:8c:d7:c7:40:d7:5a:
    73:23:23:a0:09:6e:2e:98:da:e3:42:4c:76:64:72:
    ed:08:e1:5b:4b:c1:ba:cc:f8:6f:82:c8:55:90:3b:
    ef:78:f5:07:ff:56:ab:d1:ba:32:f6:95:28:65:7f:
    0a:50:45:00:6e:b7:d8:d9:80:83:e6:3b:10:09:d5:
    e1:3f:b6:b1:6e:58:f5:10:c2:79:8a:6b:5a:6f:17:
    40:49:51:92:46:e2:a0:e7:67:ae:7d:99:01:88:f2:
    53:6e:72:c9:4e:32:cf:41:7f:5a:53:f7:cf:b0:59:
    46:69:43:44:0d:1d:8e:6a:5f
```

```
prime2:
    00:e2:09:42:ea:89:6d:43:66:c5:88:c5:16:d3:2c:
    3e:5f:df:ba:19:0e:e4:a7:b3:60:db:ec:2d:e6:2f:
    8b:d6:3a:fc:f3:1d:c3:be:61:36:fd:c6:2e:eb:a6:
    83:a7:cd:cc:af:67:98:ef:16:84:19:78:d9:dd:e7:
    cb:d9:51:29:3a:29:19:cb:14:3a:c3:ad:0b:11:e7:
    f3:d3:34:b2:f0:49:48:c7:31:ea:a7:d7:52:63:56:
    7c:fd:6e:4f:1c:94:ac:09:86:3c:22:e3:c1:71:66:
    06:1e:d4:b3:80:27:3b:47:22:6b:3d:02:d1:40:64:
    91:5a:e5:39:a7:c6:8a:35:81
```

Private exponent, d:

```
privateExponent:
    00:b4:f3:86:e0:b2:c1:bb:40:45:08:7a:1a:c9:a8:
    c3:a0:f2:85:5f:70:b3:be:74:db:81:94:9d:25:d8:
    e4:3d:2c:03:2f:6e:53:7e:5e:1d:74:31:5f:c4:a0:
    cd:dc:7a:b1:21:8d:05:c8:32:84:49:bf:8e:cb:8f:
    ca:a7:44:a2:57:7f:48:f3:54:68:ae:82:b9:0e:50:
    b5:cb:f2:62:dd:c7:93:31:75:78:f1:44:45:d7:2b:
    3d:7d:89:67:45:29:31:df:e4:ac:25:b0:41:0d:d2:
    a0:de:73:30:56:1d:ce:21:e0:ad:a7:90:b0:e8:22:
    34:c4:8b:9c:8d:53:b1:13:57:af:2a:40:92:6c:bb:
    c8:be:1c:0c:81:e9:23:96:e8:57:3e:56:f0:ef:98:
    82:17:22:51:5e:d0:3f:a0:d8:fe:58:d5:cc:30:73:
    a0:9f:10:30:ea:53:4d:13:bc:d9:b4:76:81:11:07:
    cb:cb:2a:88:89:d2:57:cd:cb:cd:48:e6:70:58:4a:
    8b:d7:f1:36:db:a2:ed:32:6e:cf:58:5a:c5:51:03:
    52:1b:76:bd:d0:03:d7:da:bc:ae:33:bc:cc:94:01:
    8e:81:0b:96:04:c7:d7:42:d8:99:66:9a:cf:3b:71:
    f5:1c:32:a7:c4:19:d7:b6:34:74:6a:c6:b7:3c:67:
    bc:01
```

Step 2. In this step, a web server creates a public/private key pair and requests for a certificate from the CA we have created.

1. The web server securitylab2022.com generates public/private key pair:

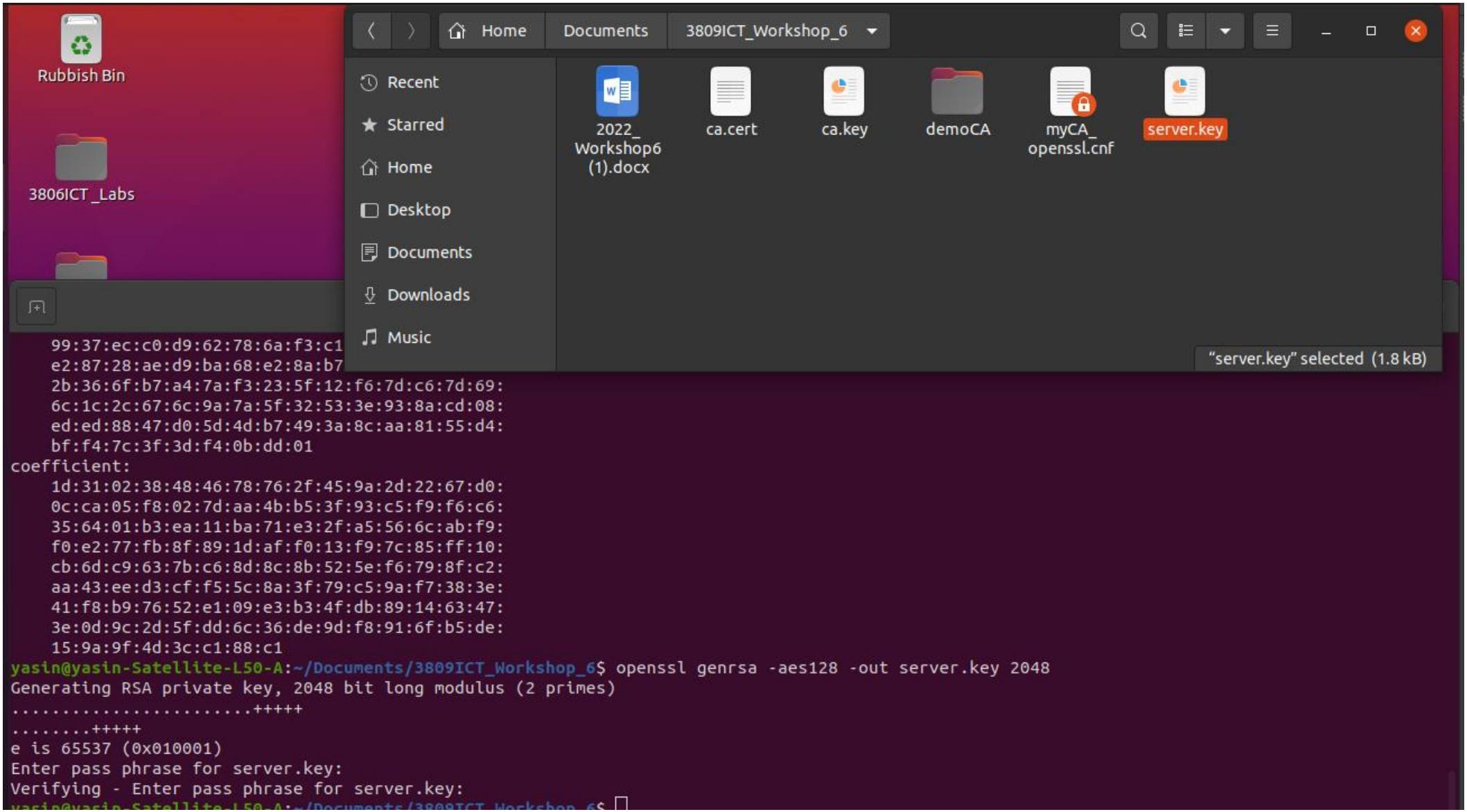
   $ openssl genrsa -aes128 -out server.key 2048

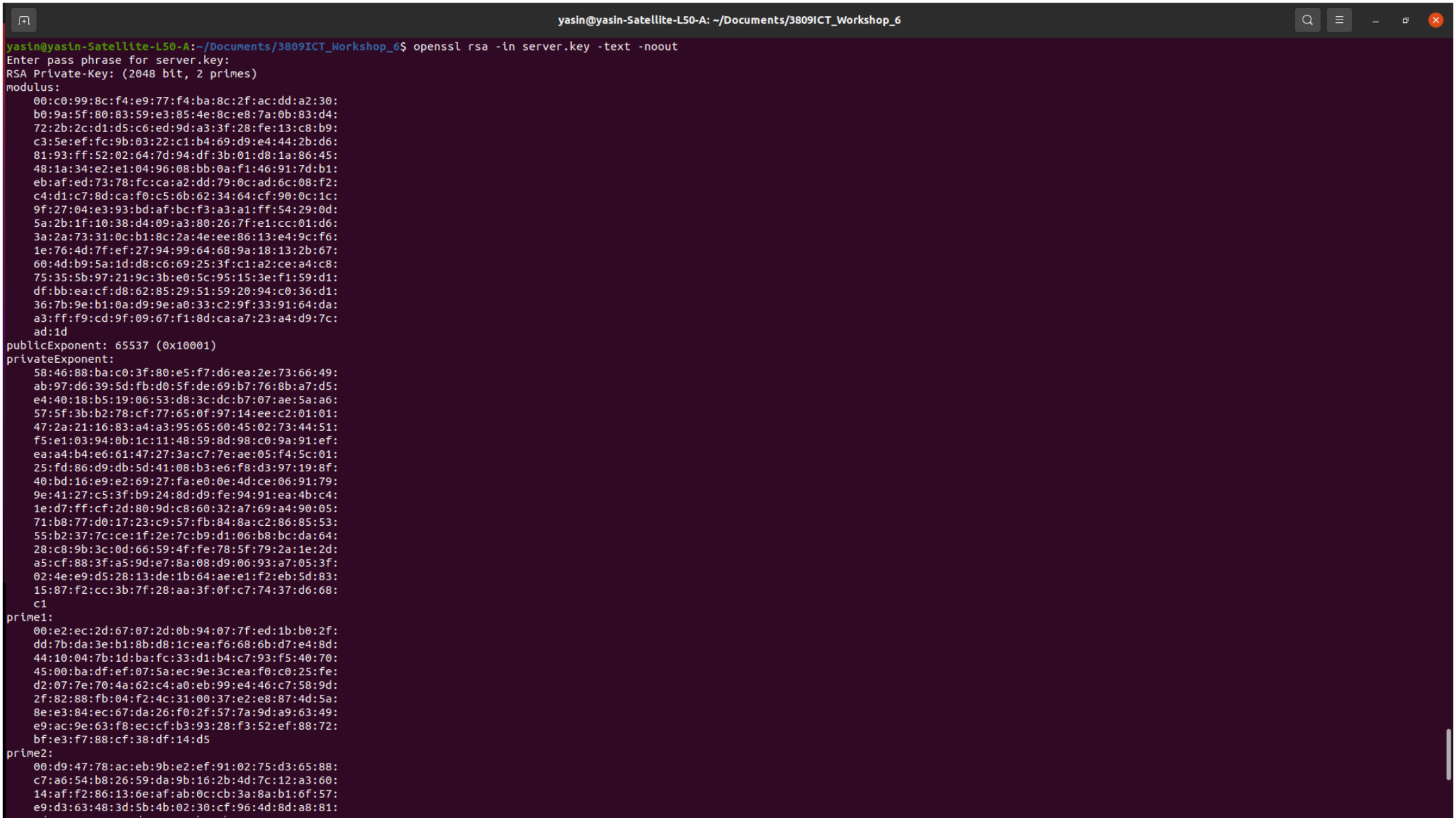
   and we can see the key values via

   $ openssl rsa -in server.key -text -noout

   Again, you should notice that a special number 65537 (10001 in hexadecimal) is chosen for the public (verification) exponent *e*.

   Answer:


Rubbish Bin
3806ICT_Labs
Home
Documents
3809ICT_Workshop_6
Recent
Starred
Home
Desktop
Documents
Downloads
Music
2022_ Workshop6 (1).docx
ca.cert
ca.key
demoCA
myCA_ openssl.cnf
server.key
"server.key" selected (1.8 kB)
99:37:ec:c0:d9:62:78:6a:f3:c1
e2:87:28:ae:d9:ba:68:e2:8a:b7
2b:36:6f:b7:a4:7a:f3:23:5f:12:f6:7d:c6:7d:69:
6c:1c:2c:67:6c:9a:7a:5f:32:53:3e:93:8a:cd:08:
ed:ed:88:47:d0:5d:4d:b7:49:3a:8c:aa:81:55:d4:
bf:f4:7c:3f:3d:f4:0b:dd:01
coefficient:
1d:31:02:38:48:46:78:76:2f:45:9a:2d:22:67:d0:
0c:ca:05:f8:02:7d:aa:4b:b5:3f:93:c5:f9:f6:c6:
35:64:01:b3:ea:11:ba:71:e3:2f:a5:56:6c:ab:f9:
f0:e2:77:fb:8f:89:1d:af:f0:13:f9:7c:85:ff:10:
cb:6d:c9:63:7b:c6:8d:8c:8b:52:5e:f6:79:8f:c2:
aa:43:ee:d3:cf:f5:5c:8a:3f:79:c5:9a:f7:38:3e:
41:f8:b9:76:52:e1:09:e3:b3:4f:db:89:14:63:47:
3e:0d:9c:2d:5f:dd:6c:36:de:9d:f8:91:6f:b5:de:
15:9a:9f:4d:3c:c1:88:c1
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl genrsa -aes128 -out server.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl rsa -in server.key -text -noout
Enter pass phrase for server.key:
RSA Private-Key: (2048 bit, 2 primes)
modulus:
00:c0:99:8c:f4:e9:77:f4:ba:8c:2f:ac:dd:a2:30:
b0:9a:5f:80:83:59:e3:85:4e:8c:e8:7a:0b:83:d4:
72:2b:2c:d1:d5:c6:ed:9d:a3:3f:28:fe:13:c8:b9:
c3:5e:ef:fc:9b:03:22:c1:b4:69:d9:e4:44:2b:d6:
81:93:ff:52:02:64:7d:94:df:3b:01:d8:1a:86:45:
48:1a:34:e2:e1:04:96:08:bb:0a:f1:46:91:7d:b1:
eb:af:ed:73:78:fc:ca:a2:dd:79:0c:ad:6c:08:f2:
c4:d1:c7:8d:ca:f0:c5:6b:62:34:64:cf:90:0c:1c:
9f:27:04:e3:93:bd:af:bc:f3:a3:a1:ff:54:29:0d:
5a:2b:1f:10:38:d4:09:a3:80:26:7f:e1:cc:01:d6:
3a:2a:73:31:0c:b1:8c:2a:4e:ee:86:13:e4:9c:f6:
1e:76:4d:7f:ef:27:94:99:64:68:9a:18:13:2b:67:
60:4d:b9:5a:1d:d8:c6:69:25:3f:c1:a2:ce:a4:c8:
75:35:5b:97:21:9c:3b:e0:5c:95:15:3e:f1:59:d1:
df:bb:ea:cf:d8:62:85:29:51:59:20:94:c0:36:d1:
36:7b:9e:b1:0a:d9:9e:a0:33:c2:9f:33:91:64:da:
a3:ff:f9:cd:9f:09:67:f1:8d:ca:a7:23:a4:d9:7c:
ad:1d
publicExponent: 65537 (0x10001)
privateExponent:
58:46:88:ba:c0:3f:80:e5:f7:d6:ea:2e:73:66:49:
ab:97:d6:39:5d:fb:d0:5f:de:69:b7:76:8b:a7:d5:
e4:40:18:b5:19:06:53:d8:3c:dc:b7:07:ae:5a:a6:
57:5f:3b:b2:78:cf:77:65:0f:97:14:ee:c2:01:01:
47:2a:21:16:83:a4:a3:95:65:60:45:02:73:44:51:
f5:e1:03:94:0b:1c:11:48:59:8d:98:c0:9a:91:ef:
ea:a4:b4:e6:61:47:27:3a:c7:7e:ae:05:f4:5c:01:
25:fd:86:d9:db:5d:41:08:b3:e6:f8:d3:97:19:8f:
40:bd:16:e9:e2:69:27:fa:e0:0e:4d:ce:06:91:79:
9e:41:27:c5:3f:b9:24:8d:d9:fe:94:91:ea:4b:c4:
1e:d7:ff:cf:2d:80:9d:c8:60:32:a7:69:a4:90:05:
71:b8:77:d0:17:23:c9:57:fb:84:8a:c2:86:85:53:
55:b2:37:7c:ce:1f:2e:7c:b9:d1:06:b8:bc:da:64:
28:c8:9b:3c:0d:66:59:4f:fe:78:5f:79:2a:1e:2d:
a5:cf:88:3f:a5:9d:e7:8a:08:d9:06:93:a7:05:3f:
02:4e:e9:d5:28:13:de:1b:64:ae:e1:f2:eb:5d:83:
15:87:f2:cc:3b:7f:28:aa:3f:0f:c7:74:37:d6:68:
c1
prime1:
00:e2:ec:2d:67:07:2d:0b:94:07:7f:ed:1b:b0:2f:
dd:7b:da:3e:b1:8b:d8:1c:ea:f6:68:6b:d7:e4:8d:
44:10:04:7b:1d:ba:fc:33:d1:b4:c7:93:f5:40:70:
45:00:ba:df:ef:07:5a:ec:9e:3c:ea:f0:c0:25:fe:
d2:07:7e:70:4a:62:c4:a0:eb:99:e4:46:c7:58:9d:
2f:82:88:fb:04:f2:4c:31:00:37:e2:e8:87:4d:5a:
8e:e3:84:ec:67:da:26:f0:2f:57:7a:9d:a9:63:49:
e9:ac:9e:63:f8:ec:cf:b3:93:28:f3:52:ef:88:72:
bf:e3:f7:88:cf:38:df:14:d5
prime2:
00:d9:47:78:ac:eb:9b:e2:ef:91:02:75:d3:65:88:
c7:a6:54:b8:26:59:da:9b:16:2b:4d:7c:12:a3:60:
14:af:f2:86:13:6e:af:ab:0c:cb:3a:8a:b1:6f:57:
e9:d3:63:48:3d:5b:4b:02:30:cf:96:4d:8d:a8:81:

```
    55:b2:37:7c:ce:1f:2e:7c:b9:d1:06:b8:bc:da:64:
    28:c8:9b:3c:0d:66:59:4f:fe:78:5f:79:2a:1e:2d:
    a5:cf:88:3f:a5:9d:e7:8a:08:d9:06:93:a7:05:3f:
    02:4e:e9:d5:28:13:de:1b:64:ae:e1:f2:eb:5d:83:
    15:87:f2:cc:3b:7f:28:aa:3f:0f:c7:74:37:d6:68:
    c1
prime1:
    00:e2:ec:2d:67:07:2d:0b:94:07:7f:ed:1b:b0:2f:
    dd:7b:da:3e:b1:8b:d8:1c:ea:f6:68:6b:d7:e4:8d:
    44:10:04:7b:1d:ba:fc:33:d1:b4:c7:93:f5:40:70:
    45:00:ba:df:ef:07:5a:ec:9e:3c:ea:f0:c0:25:fe:
    d2:07:7e:70:4a:62:c4:a0:eb:99:e4:46:c7:58:9d:
    2f:82:88:fb:04:f2:4c:31:00:37:e2:e8:87:4d:5a:
    8e:e3:84:ec:67:da:26:f0:2f:57:7a:9d:a9:63:49:
    e9:ac:9e:63:f8:ec:cf:b3:93:28:f3:52:ef:88:72:
    bf:e3:f7:88:cf:38:df:14:d5
prime2:
    00:d9:47:78:ac:eb:9b:e2:ef:91:02:75:d3:65:88:
    c7:a6:54:b8:26:59:da:9b:16:2b:4d:7c:12:a3:60:
    14:af:f2:86:13:6e:af:ab:0c:cb:3a:8a:b1:6f:57:
    e9:d3:63:48:3d:5b:4b:02:30:cf:96:4d:8d:a8:81:
    ad:78:8a:a5:4c:d9:13:6a:b7:cb:0a:08:e6:26:a7:
    0e:aa:77:b1:41:27:ee:c0:1a:2b:73:65:3f:35:4f:
    29:22:b9:d0:b3:be:7a:aa:de:22:30:82:e3:36:a1:
    8c:b9:b8:01:8a:12:59:1f:00:17:f1:e7:35:70:aa:
    b7:ad:3a:0e:bd:b3:c0:7b:29
exponent1:
    00:d5:56:d1:c0:a1:00:7a:78:2b:2c:dc:10:41:ee:
    5e:3e:48:8a:d4:84:f3:23:0c:cb:a8:94:6b:1e:96:
    a9:3c:9d:d9:d9:b3:a7:d4:57:fd:ab:fc:b0:80:6a:
    8c:95:09:1b:eb:2f:71:0e:30:1e:79:8a:ea:3b:4e:
    7c:cb:4a:d5:eb:39:3c:3f:46:01:22:9a:60:64:31:
    33:2f:77:f4:f7:4b:8c:d2:2c:b0:5e:05:da:de:a0:
    9a:e1:d0:60:29:aa:f1:1c:b2:85:7d:e3:a8:12:8e:
    b4:bf:f3:11:6e:3f:c5:6d:c0:96:a9:5c:79:92:40:
    bf:a3:65:5f:1b:e3:0d:e8:19
exponent2:
    00:9c:fd:3e:fb:f1:e0:58:3f:b0:0e:8f:03:86:c1:
    25:3f:d0:c6:9d:2f:1e:fc:1f:30:7a:73:c3:23:b8:
    30:3a:50:88:ff:51:62:2b:bc:ba:ba:39:ab:aa:3f:
    62:fb:11:29:08:ec:05:6e:37:c6:45:5b:13:97:44:
    db:09:d5:63:49:fb:2e:44:55:37:a6:b0:77:5a:46:
    2a:1a:91:10:c9:7b:08:ce:54:1a:40:ee:4e:95:3d:
    f5:02:da:2f:29:2f:df:81:c5:ad:fe:4f:13:cc:4d:
    3d:58:92:d2:c9:e8:27:ec:76:2c:d6:e3:af:81:10:
    58:56:19:34:bd:6c:3b:0e:c1
coefficient:
    00:91:24:e0:0e:d1:4d:2c:33:69:fb:6b:86:16:15:
    60:df:50:8f:54:59:ec:14:14:89:a6:18:14:99:e6:
    9a:3f:25:c4:69:a4:4e:83:9b:96:65:43:b6:6b:9e:
    e8:a9:d5:52:47:2d:35:7a:c8:54:d9:70:83:f6:04:
    2d:76:e4:4c:50:4f:da:4c:69:b8:32:75:b3:bc:9f:
    a5:1b:33:31:5d:e1:86:e8:69:17:db:53:8d:6e:e5:
    39:f4:f6:79:db:f4:19:e8:23:fe:fb:ba:f0:06:b5:
    2a:29:7b:90:17:c2:45:ef:d5:24:88:f8:09:53:6c:
    d5:0f:19:bc:6e:3b:ad:0a:1d
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$
```

2. Server securitylab2022.com requests certificate from CA by generating a Certificate Signing Request (CSR). Note that the public key from server.key has not been signed (certified). Therefore, no one would trust and use such public key to perform encryption or verification. The server needs to send it to CA for being certified. To this end, the server sends out a request.

   You need to supply the pass phrase for server.key with which the CA can open server.key and sign it. You also supply information to the server. What will happen in reality is that CA will check this information against your actually information. If what you supplied are authentic, CA will certify the server's key.

   ```
   $ openssl req -new -key server.key -out server.csr -config
   myCA_openssl.cnf
   ```

   You need correctly apply the password for server.key (as it was protected by a password). After entering below password, please fill out fields as below and the other fields with anything you want.

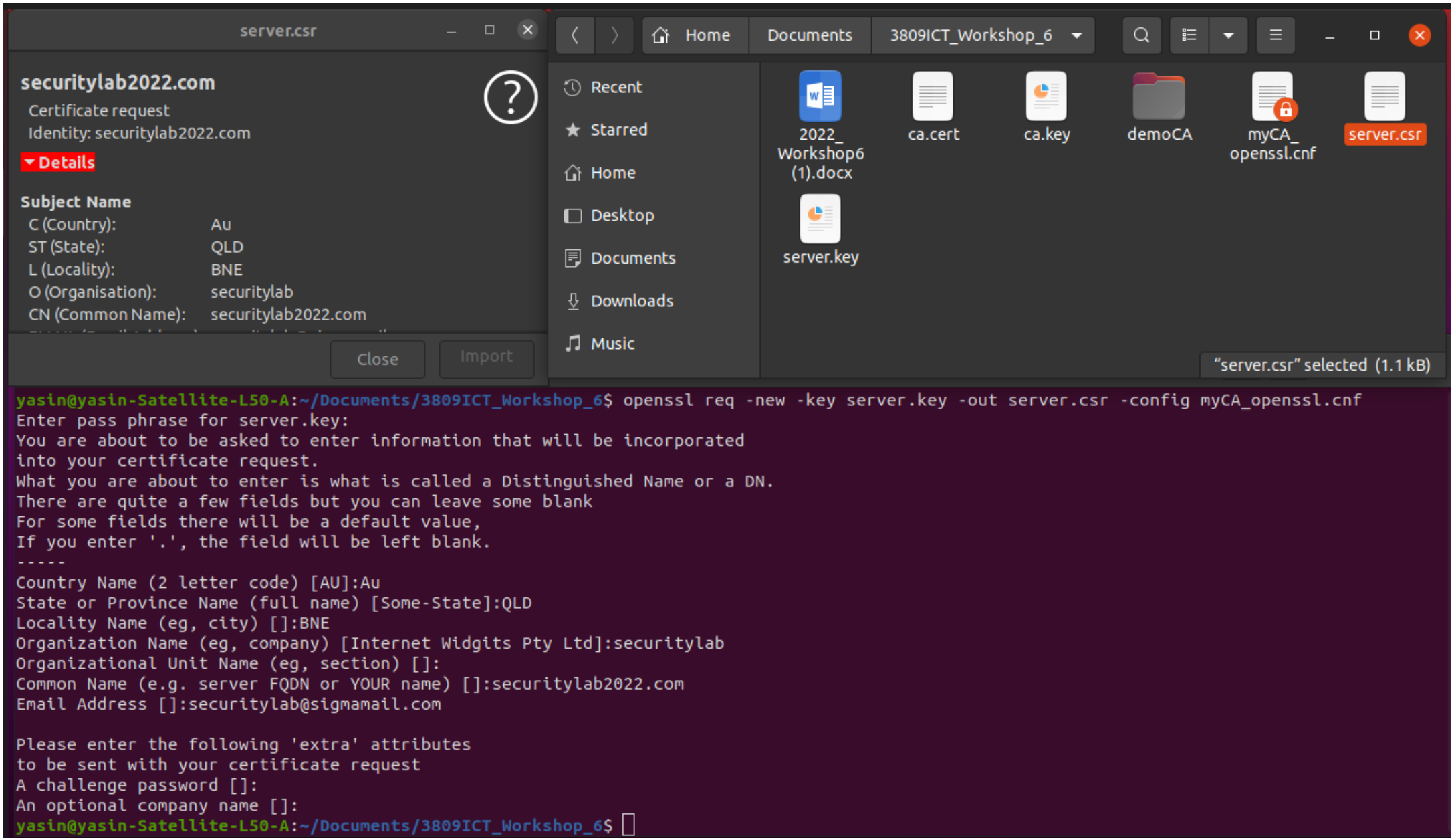
   ```
   Country Name = AU
   State Or Province Name = QLD
   Organization Name = securitylab
   Common Name = securitylab2022.com
   ```

   The file server.csr is the request output and it contains the server's public key and server supplied information. To see the content of server.csr, you can use the following command:

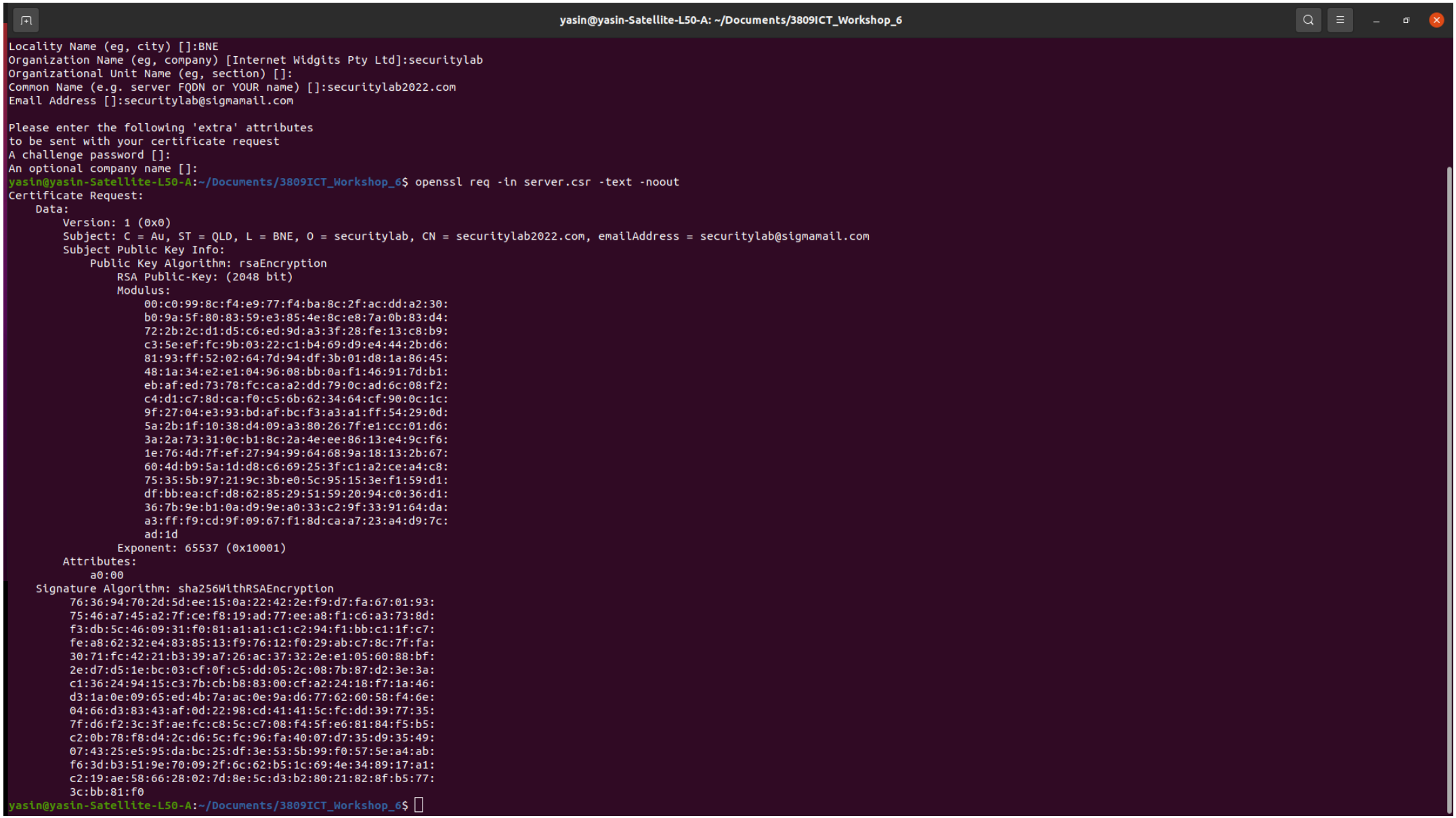
   ```
   $ openssl req -in server.csr -text -noout
   ```

   Answer:

   Answer


server.csr
securitylab2022.com
Certificate request
Identity: securitylab2022.com
Details
Subject Name
C (Country): Au
ST (State): QLD
L (Locality): BNE
O (Organisation): securitylab
CN (Common Name): securitylab2022.com
Close
Import
Home
Documents
3809ICT_Workshop_6
Recent
Starred
Home
Desktop
Documents
Downloads
Music
2022_ Workshop6 (1).docx
ca.cert
ca.key
demoCA
myCA_ openssl.cnf
server.csr
server.key
"server.csr" selected (1.1 kB)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl req -new -key server.key -out server.csr -config myCA_openssl.cnf
Enter pass phrase for server.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]:Au
State or Province Name (full name) [Some-State]:QLD
Locality Name (eg, city) []:BNE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:securitylab
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:securitylab2022.com
Email Address []:securitylab@sigmamail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
Locality Name (eg, city) []:BNE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:securitylab
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:securitylab2022.com
Email Address []:securitylab@sigmamail.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl req -in server.csr -text -noout
Certificate Request:
Data:
Version: 1 (0x0)
Subject: C = Au, ST = QLD, L = BNE, O = securitylab, CN = securitylab2022.com, emailAddress = securitylab@sigmamail.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:c0:99:8c:f4:e9:77:f4:ba:8c:2f:ac:dd:a2:30:
b0:9a:5f:80:83:59:e3:85:4e:8c:e8:7a:0b:83:d4:
72:2b:2c:d1:d5:c6:ed:9d:a3:3f:28:fe:13:c8:b9:
c3:5e:ef:fc:9b:03:22:c1:b4:69:d9:e4:44:2b:d6:
81:93:ff:52:02:64:7d:94:df:3b:01:d8:1a:86:45:
48:1a:34:e2:e1:04:96:08:bb:0a:f1:46:91:7d:b1:
eb:af:ed:73:78:fc:ca:a2:dd:79:0c:ad:6c:08:f2:
c4:d1:c7:8d:ca:f0:c5:6b:62:34:64:cf:90:0c:1c:
9f:27:04:e3:93:bd:af:bc:f3:a3:a1:ff:54:29:0d:
5a:2b:1f:10:38:d4:09:a3:80:26:7f:e1:cc:01:d6:
3a:2a:73:31:0c:b1:8c:2a:4e:ee:86:13:e4:9c:f6:
1e:76:4d:7f:ef:27:94:99:64:68:9a:18:13:2b:67:
60:4d:b9:5a:1d:d8:c6:69:25:3f:c1:a2:ce:a4:c8:
75:35:5b:97:21:9c:3b:e0:5c:95:15:3e:f1:59:d1:
df:bb:ea:cf:d8:62:85:29:51:59:20:94:c0:36:d1:
36:7b:9e:b1:0a:d9:9e:a0:33:c2:9f:33:91:64:da:
a3:ff:f9:cd:9f:09:67:f1:8d:ca:a7:23:a4:d9:7c:
ad:1d
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: sha256WithRSAEncryption
76:36:94:70:2d:5d:ee:15:0a:22:42:2e:f9:d7:fa:67:01:93:
75:46:a7:45:a2:7f:ce:f8:19:ad:77:ee:a8:f1:c6:a3:73:8d:
f3:db:5c:46:09:31:f0:81:a1:a1:c1:c2:94:f1:bb:c1:1f:c7:
fe:a8:62:32:e4:83:85:13:f9:76:12:f0:29:ab:c7:8c:7f:fa:
30:71:fc:42:21:b3:39:a7:26:ac:37:32:2e:e1:05:60:88:bf:
2e:d7:d5:1e:bc:03:cf:0f:c5:dd:05:2c:08:7b:87:d2:3e:3a:
c1:36:24:94:15:c3:7b:cb:b8:83:00:cf:a2:24:18:f7:1a:46:
d3:1a:0e:09:65:ed:4b:7a:ac:0e:9a:d6:77:62:60:58:f4:6e:
04:66:d3:83:43:af:0d:22:98:cd:41:41:5c:fc:dd:39:77:35:
7f:d6:f2:3c:3f:ae:fc:c8:5c:c7:08:f4:5f:e6:81:84:f5:b5:
c2:0b:78:f8:d4:2c:d6:5c:fc:96:fa:40:07:d7:35:d9:35:49:
07:43:25:e5:95:da:bc:25:df:3e:53:5b:99:f0:57:5e:a4:ab:
f6:3d:b3:51:9e:70:09:2f:6c:62:b5:1c:69:4e:34:89:17:a1:
c2:19:ae:58:66:28:02:7d:8e:5c:d3:b2:80:21:82:8f:b5:77:
3c:bb:81:f0
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$

Q: Note, the CSR must prove to the CA that the server indeed knows the corresponding private key, i.e., the public key indeed belongs to the server securitylab2022.com. Looking at the content of server.csr, how does the server.csr proves that it knows the private key?

Answer:
The CA will verify the signature using the server's public key as the signature can only be produced by a private key.

3. After received server.csr, CA checks the information and produces a digital certificate for securitylab2022.com. To this end, CA uses its own certificate (which contains it public key) and its private signing key ca.key. Note, since CA is universally trusted (in the domain), there is no need for a further proof of the correspondence between the CA's public key ca.crt and CA's.

```
$ openssl ca -in server.csr -out server.cert -cert ca.cert /
-keyfile ca.key -config myCA_openssl.cnf
```

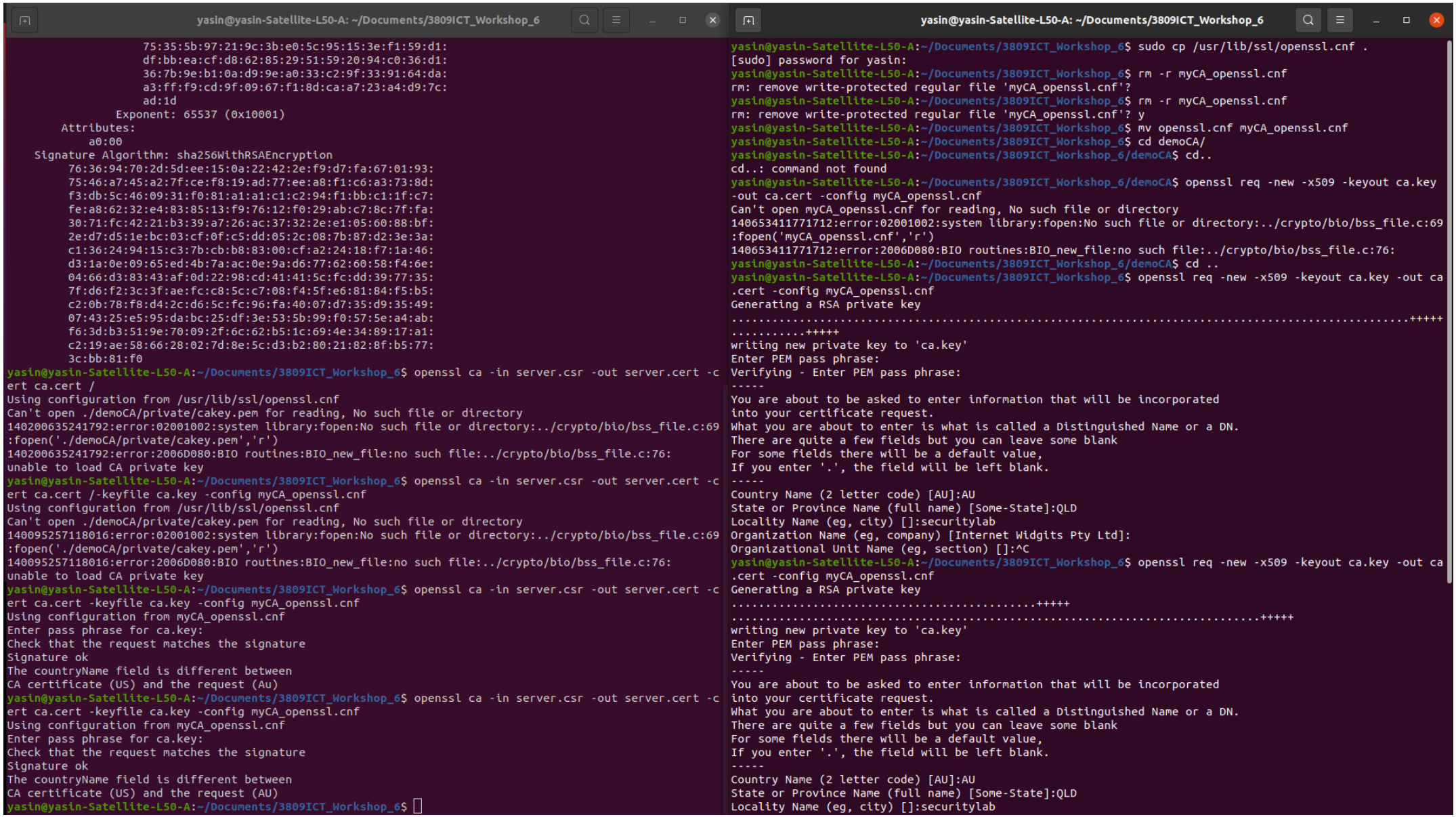
You need the pass phrase for ca.key. The output server.crt is the server's digital certificate. You can see requests pop up asking for confirming issuing the certificate. Select "y" (yes) and proceed to the next.

Answer:
In the following steps the certification failed due to details being different such as the country field, so on the terminal of the right had side show I had to recreate my self-signed certificate.

Verify(PU,M, σ) where $\sigma^e \bmod n = M$ and using this mathematical relationship

$M = (E^e)^d \bmod n$

$= E^{ed} \bmod n$
$= (E^d)^e \bmod n$ // server proves d using e and n

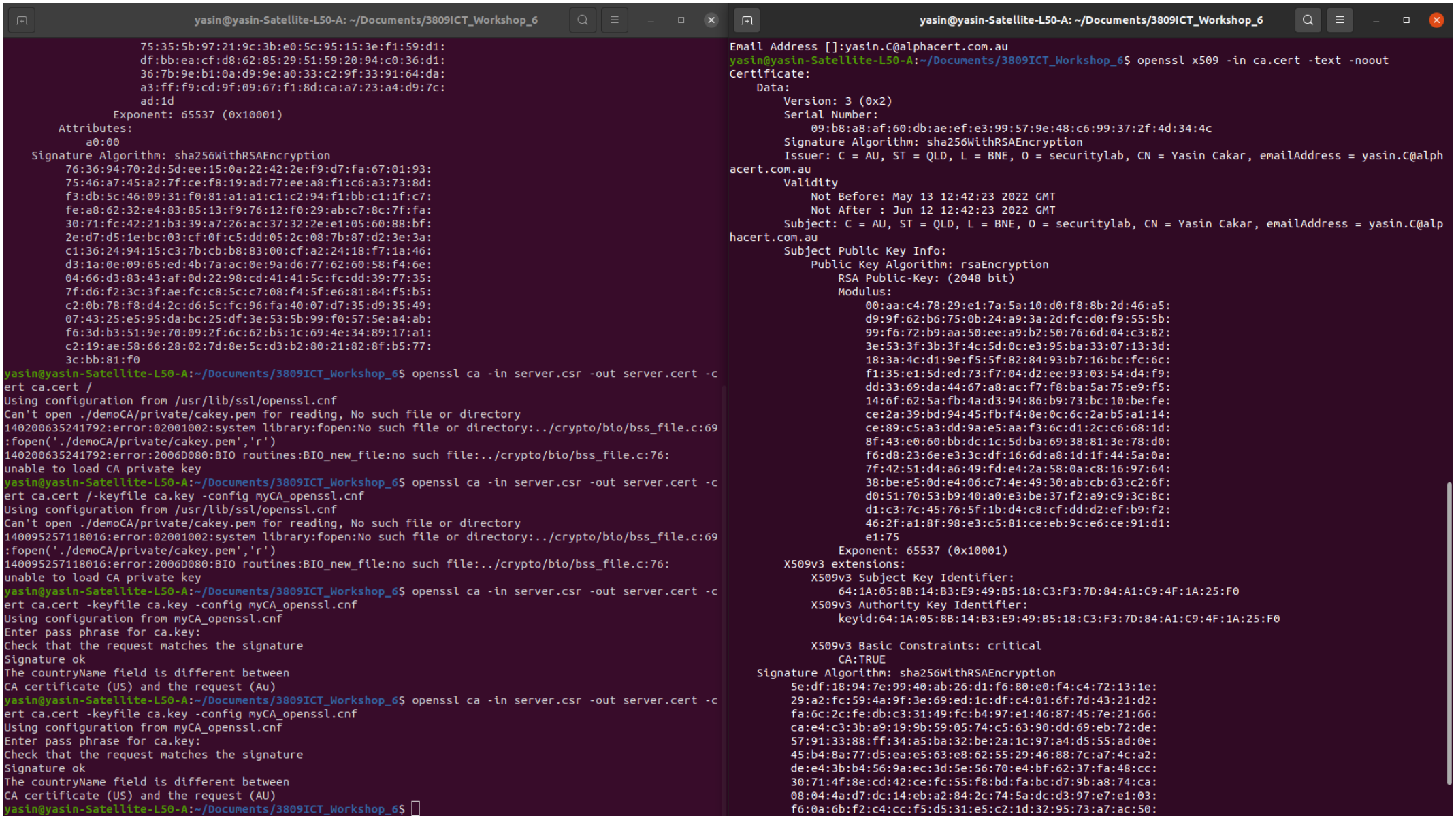

yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
75:35:5b:97:21:9c:3b:e0:5c:95:15:3e:f1:59:d1:
df:bb:ea:cf:d8:62:85:29:51:59:20:94:c0:36:d1:
36:7b:9e:b1:0a:d9:9e:a0:33:c2:9f:33:91:64:da:
a3:ff:f9:cd:9f:09:67:f1:8d:ca:a7:23:a4:d9:7c:
ad:1d
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: sha256WithRSAEncryption
76:36:94:70:2d:5d:ee:15:0a:22:42:2e:f9:d7:fa:67:01:93:
75:46:a7:45:a2:7f:ce:f8:19:ad:77:ee:a8:f1:c6:a3:73:8d:
f3:db:5c:46:09:31:f0:81:a1:a1:c1:c2:94:f1:bb:c1:1f:c7:
fe:a8:62:32:e4:83:85:13:f9:76:12:f0:29:ab:c7:8c:7f:fa:
30:71:fc:42:21:b3:39:a7:26:ac:37:32:2e:e1:05:60:88:bf:
2e:d7:d5:1e:bc:03:cf:0f:c5:dd:05:2c:08:7b:87:d2:3e:3a:
c1:36:24:94:15:c3:7b:cb:b8:83:00:cf:a2:24:18:f7:1a:46:
d3:1a:0e:09:65:ed:4b:7a:ac:0e:9a:d6:77:62:60:58:f4:6e:
04:66:d3:83:43:af:0d:22:98:cd:41:41:5c:fc:dd:39:77:35:
7f:d6:f2:3c:3f:ae:fc:c8:5c:c7:08:f4:5f:e6:81:84:f5:b5:
c2:0b:78:f8:d4:2c:d6:5c:fc:96:fa:40:07:d7:35:d9:35:49:
07:43:25:e5:95:da:bc:25:df:3e:53:5b:99:f0:57:5e:a4:ab:
f6:3d:b3:51:9e:70:09:2f:6c:62:b5:1c:69:4e:34:89:17:a1:
c2:19:ae:58:66:28:02:7d:8e:5c:d3:b2:80:21:82:8f:b5:77:
3c:bb:81:f0
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert /
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140200635241792:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69
:fopen('./demoCA/private/cakey.pem','r')
140200635241792:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert /-keyfile ca.key -config myCA_openssl.cnf
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140095257118016:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69
:fopen('./demoCA/private/cakey.pem','r')
140095257118016:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (Au)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (AU)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ sudo cp /usr/lib/ssl/openssl.cnf .
[sudo] password for yasin:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ rm -r myCA_openssl.cnf
rm: remove write-protected regular file 'myCA_openssl.cnf'?
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ rm -r myCA_openssl.cnf
rm: remove write-protected regular file 'myCA_openssl.cnf'? y
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ mv openssl.cnf myCA_openssl.cnf
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ cd demoCA/
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ cd..
cd..: command not found
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ openssl req -new -x509 -keyout ca.key
-out ca.cert -config myCA_openssl.cnf
Can't open myCA_openssl.cnf for reading, No such file or directory
140653411771712:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69
:fopen('myCA_openssl.cnf','r')
140653411771712:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6/demoCA$ cd ..
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl req -new -x509 -keyout ca.key -out ca
.cert -config myCA_openssl.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

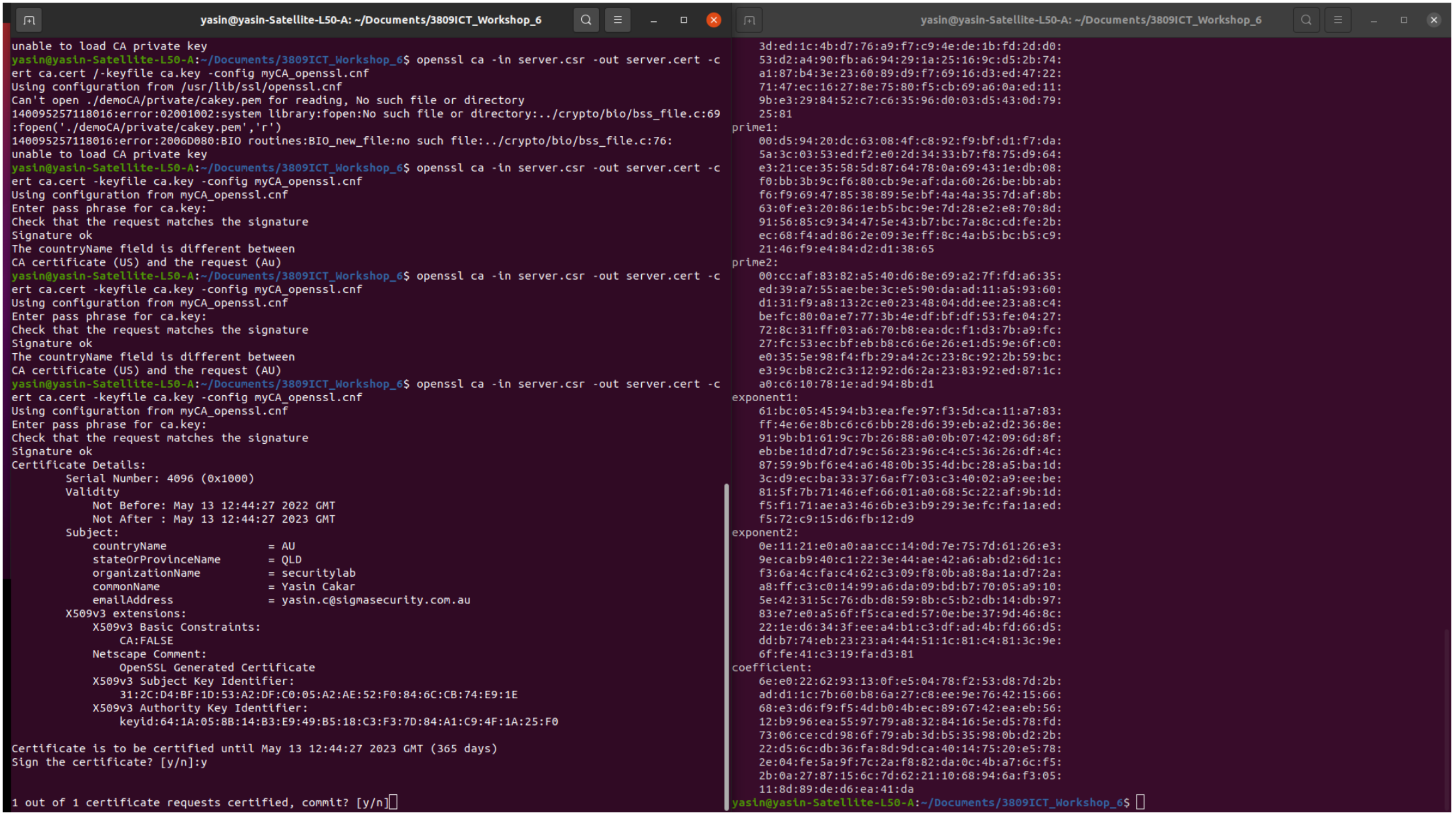
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

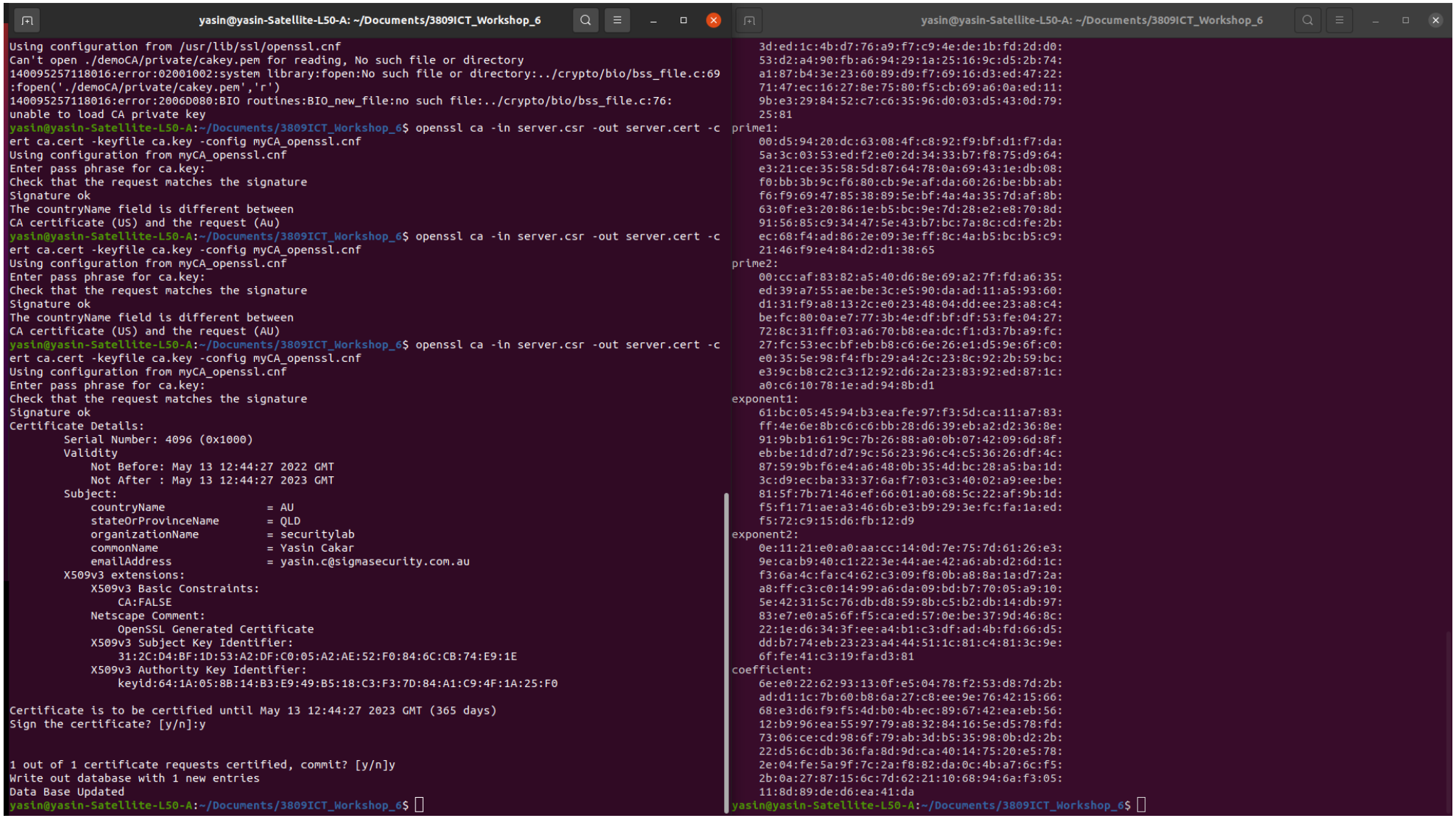
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:QLD
Locality Name (eg, city) []:securitylab
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:^C
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl req -new -x509 -keyout ca.key -out ca
.cert -config myCA_openssl.cnf
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
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.

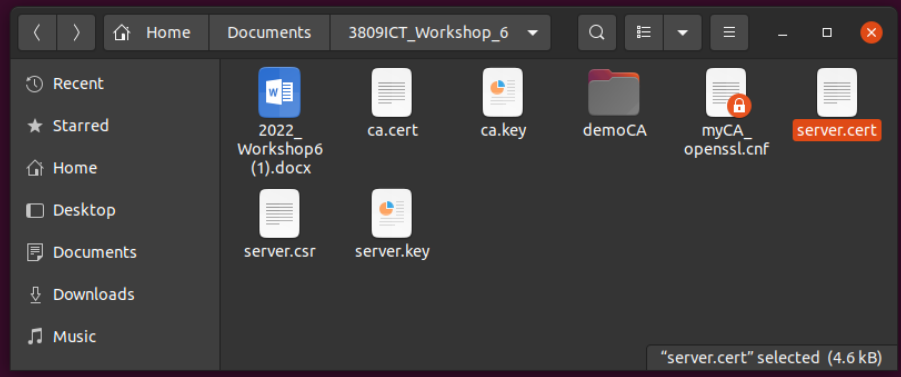
Country Name (2 letter code) [AU]:AU
State or Province Name (full name) [Some-State]:QLD
Locality Name (eg, city) []:securitylab


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
75:35:5b:97:21:9c:3b:e0:5c:95:15:3e:f1:59:d1:
df:bb:ea:cf:d8:62:85:29:51:59:20:94:c0:36:d1:
36:7b:9e:b1:0a:d9:9e:a0:33:c2:9f:33:91:64:da:
a3:ff:f9:cd:9f:09:67:f1:8d:ca:a7:23:a4:d9:7c:
ad:1d
Exponent: 65537 (0x10001)
Attributes:
a0:00
Signature Algorithm: sha256WithRSAEncryption
76:36:94:70:2d:5d:ee:15:0a:22:42:2e:f9:d7:fa:67:01:93:
75:46:a7:45:a2:7f:ce:f8:19:ad:77:ee:a8:f1:c6:a3:73:8d:
f3:db:5c:46:09:31:f0:81:a1:a1:c1:c2:94:f1:bb:c1:1f:c7:
fe:a8:62:32:e4:83:85:13:f9:76:12:f0:29:ab:c7:8c:7f:fa:
30:71:fc:42:21:b3:39:a7:26:ac:37:32:2e:e1:05:60:88:bf:
2e:d7:d5:1e:bc:03:cf:0f:c5:dd:05:2c:08:7b:87:d2:3e:3a:
c1:36:24:94:15:c3:7b:cb:b8:83:00:cf:a2:24:18:f7:1a:46:
d3:1a:0e:09:65:ed:4b:7a:ac:0e:9a:d6:77:62:60:58:f4:6e:
04:66:d3:83:43:af:0d:22:98:cd:41:41:5c:fc:dd:39:77:35:
7f:d6:f2:3c:3f:ae:fc:c8:5c:c7:08:f4:5f:e6:81:84:f5:b5:
c2:0b:78:f8:d4:2c:d6:5c:fc:96:fa:40:07:d7:35:d9:35:49:
07:43:25:e5:95:da:bc:25:df:3e:53:5b:99:f0:57:5e:a4:ab:
f6:3d:b3:51:9e:70:09:2f:6c:62:b5:1c:69:4e:34:89:17:a1:
c2:19:ae:58:66:28:02:7d:8e:5c:d3:b2:80:21:82:8f:b5:77:
3c:bb:81:f0
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert /
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140200635241792:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('./demoCA/private/cakey.pem','r')
140200635241792:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert /-keyfile ca.key -config myCA_openssl.cnf
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140095257118016:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('./demoCA/private/cakey.pem','r')
140095257118016:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (Au)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (AU)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
Email Address []:yasin.C@alphacert.com.au
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl x509 -in ca.cert -text -noout
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
09:b8:a8:af:60:db:ae:ef:e3:99:57:9e:48:c6:99:37:2f:4d:34:4c
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = AU, ST = QLD, L = BNE, O = securitylab, CN = Yasin Cakar, emailAddress = yasin.C@alphacert.com.au
Validity
Not Before: May 13 12:42:23 2022 GMT
Not After : Jun 12 12:42:23 2022 GMT
Subject: C = AU, ST = QLD, L = BNE, O = securitylab, CN = Yasin Cakar, emailAddress = yasin.C@alphacert.com.au
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:aa:c4:78:29:e1:7a:5a:10:d0:f8:8b:2d:46:a5:
d9:9f:62:b6:75:0b:24:a9:3a:2d:fc:d0:f9:55:5b:
99:f6:72:b9:aa:50:ee:a9:b2:50:76:6d:04:c3:82:
3e:53:3f:3b:3f:4c:5d:0c:e3:95:ba:33:07:13:3d:
18:3a:4c:d1:9e:f5:5f:82:84:93:b7:16:bc:fc:6c:
f1:35:e1:5d:ed:73:f7:04:d2:ee:93:03:54:d4:f9:
dd:33:69:da:44:67:a8:ac:f7:f8:ba:5a:75:e9:f5:
14:6f:62:5a:fb:4a:d3:94:86:b9:73:bc:10:be:fe:
ce:2a:39:bd:94:45:fb:f4:8e:0c:6c:2a:b5:a1:14:
ce:89:c5:a3:dd:9a:e5:aa:f3:6c:d1:2c:c6:68:1d:
8f:43:e0:60:bb:dc:1c:5d:ba:69:38:81:3e:78:d0:
f6:d8:23:6e:e3:3c:df:16:6d:a8:1d:1f:44:5a:0a:
7f:42:51:d4:a6:49:fd:e4:2a:58:0a:c8:16:97:64:
38:be:e5:0d:e4:06:c7:4e:49:30:ab:cb:63:c2:6f:
d0:51:70:53:b9:40:a0:e3:be:37:f2:a9:c9:3c:8c:
d1:c3:7c:45:76:5f:1b:d4:c8:cf:dd:d2:ef:b9:f2:
46:2f:a1:8f:98:e3:c5:81:ce:eb:9c:e6:ce:91:d1:
e1:75
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
64:1A:05:8B:14:B3:E9:49:B5:18:C3:F3:7D:84:A1:C9:4F:1A:25:F0
X509v3 Authority Key Identifier:
keyid:64:1A:05:8B:14:B3:E9:49:B5:18:C3:F3:7D:84:A1:C9:4F:1A:25:F0
X509v3 Basic Constraints: critical
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
5e:df:18:94:7e:99:40:ab:26:d1:f6:80:e0:f4:c4:72:13:1e:
29:a2:fc:59:4a:9f:3e:69:ed:1c:df:c4:01:6f:7d:43:21:d2:
fa:6c:2c:fe:db:c3:31:49:fc:b4:97:e1:46:87:45:7e:21:66:
ca:e4:c3:3b:a9:19:9b:59:05:74:c5:63:90:dd:69:eb:72:de:
57:91:33:88:ff:34:a5:ba:32:be:2a:1c:97:a4:d5:55:ad:0e:
45:b4:8a:77:d5:ea:e5:63:e8:62:55:29:46:88:7c:a7:4c:a2:
de:e4:3b:b4:56:9a:ec:3d:5e:56:70:e4:bf:62:37:fa:48:cc:
30:71:4f:8e:cd:42:ce:fc:55:f8:bd:fa:bc:d7:9b:a8:74:ca:
08:04:4a:d7:dc:14:eb:a2:84:2c:74:5a:dc:d3:97:e7:e1:03:
f6:0a:6b:f2:c4:cc:f5:d5:31:e5:c2:1d:32:95:73:a7:ac:50:


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert /-keyfile ca.key -config myCA_openssl.cnf
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140095257118016:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69
:fopen('./demoCA/private/cakey.pem','r')
140095257118016:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (Au)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (AU)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_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: May 13 12:44:27 2022 GMT
Not After : May 13 12:44:27 2023 GMT
Subject:
countryName = AU
stateOrProvinceName = QLD
organizationName = securitylab
commonName = Yasin Cakar
emailAddress = yasin.c@sigmasecurity.com.au
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
31:2C:D4:BF:1D:53:A2:DF:C0:05:A2:AE:52:F0:84:6C:CB:74:E9:1E
X509v3 Authority Key Identifier:
keyid:64:1A:05:8B:14:B3:E9:49:B5:18:C3:F3:7D:84:A1:C9:4F:1A:25:F0
Certificate is to be certified until May 13 12:44:27 2023 GMT (365 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
3d:ed:1c:4b:d7:76:a9:f7:c9:4e:de:1b:fd:2d:d0:
53:d2:a4:90:fb:a6:94:29:1a:25:16:9c:d5:2b:74:
a1:87:b4:3e:23:60:89:d9:f7:69:16:d3:ed:47:22:
71:47:ec:16:27:8e:75:80:f5:cb:69:a6:0a:ed:11:
9b:e3:29:84:52:c7:c6:35:96:d0:03:d5:43:0d:79:
25:81
prime1:
00:d5:94:20:dc:63:08:4f:c8:92:f9:bf:d1:f7:da:
5a:3c:03:53:ed:f2:e0:2d:34:33:b7:f8:75:d9:64:
e3:21:ce:35:58:5d:87:64:78:0a:69:43:1e:db:08:
f0:bb:3b:9c:f6:80:cb:9e:af:da:60:26:be:bb:ab:
f6:f9:69:47:85:38:89:5e:bf:4a:4a:35:7d:af:8b:
63:0f:e3:20:86:1e:b5:bc:9e:7d:28:e2:e8:70:8d:
91:56:85:c9:34:47:5e:43:b7:bc:7a:8c:cd:fe:2b:
ec:68:f4:ad:86:2e:09:3e:ff:8c:4a:b5:bc:b5:c9:
21:46:f9:e4:84:d2:d1:38:65
prime2:
00:cc:af:83:82:a5:40:d6:8e:69:a2:7f:fd:a6:35:
ed:39:a7:55:ae:be:3c:e5:90:da:ad:11:a5:93:60:
d1:31:f9:a8:13:2c:e0:23:48:04:dd:ee:23:a8:c4:
be:fc:80:0a:e7:77:3b:4e:df:bf:df:53:fe:04:27:
72:8c:31:ff:03:a6:70:b8:ea:dc:f1:d3:7b:a9:fc:
27:fc:53:ec:bf:eb:b8:c6:6e:26:e1:d5:9e:6f:c0:
e0:35:5e:98:f4:fb:29:a4:2c:23:8c:92:2b:59:bc:
e3:9c:b8:c2:c3:12:92:d6:2a:23:83:92:ed:87:1c:
a0:c6:10:78:1e:ad:94:8b:d1
exponent1:
61:bc:05:45:94:b3:ea:fe:97:f3:5d:ca:11:a7:83:
ff:4e:6e:8b:c6:c6:bb:28:d6:39:eb:a2:d2:36:8e:
91:9b:b1:61:9c:7b:26:88:a0:0b:07:42:09:6d:8f:
eb:be:1d:d7:d7:9c:56:23:96:c4:c5:36:26:df:4c:
87:59:9b:f6:e4:a6:48:0b:35:4d:bc:28:a5:ba:1d:
3c:d9:ec:ba:33:37:6a:f7:03:c3:40:02:a9:ee:be:
81:5f:7b:71:46:ef:66:01:a0:68:5c:22:af:9b:1d:
f5:f1:71:ae:a3:46:6b:e3:b9:29:3e:fc:fa:1a:ed:
f5:72:c9:15:d6:fb:12:d9
exponent2:
0e:11:21:e0:a0:aa:cc:14:0d:7e:75:7d:61:26:e3:
9e:ca:b9:40:c1:22:3e:44:ae:42:a6:ab:d2:6d:1c:
f3:6a:4c:fa:c4:62:c3:09:f8:0b:a8:8a:1a:d7:2a:
a8:ff:c3:c0:14:99:a6:da:09:bd:b7:70:05:a9:10:
5e:42:31:5c:76:db:d8:59:8b:c5:b2:db:14:db:97:
83:e7:e0:a5:6f:f5:ca:ed:57:0e:be:37:9d:46:8c:
22:1e:d6:34:3f:ee:a4:b1:c3:df:ad:4b:fd:66:d5:
dd:b7:74:eb:23:23:a4:44:51:1c:81:c4:81:3c:9e:
6f:fe:41:c3:19:fa:d3:81
coefficient:
6e:e0:22:62:93:13:0f:e5:04:78:f2:53:d8:7d:2b:
ad:d1:1c:7b:60:b8:6a:27:c8:ee:9e:76:42:15:66:
68:e3:d6:f9:f5:4d:b0:4b:ec:89:67:42:ea:eb:56:
12:b9:96:ea:55:97:79:a8:32:84:16:5e:d5:78:fd:
73:06:ce:cd:98:6f:79:ab:3d:b5:35:98:0b:d2:2b:
22:d5:6c:db:36:fa:8d:9d:ca:40:14:75:20:e5:78:
2e:04:fe:5a:9f:7c:2a:f8:82:da:0c:4b:a7:6c:f5:
2b:0a:27:87:15:6c:7d:62:21:10:68:94:6a:f3:05:
11:8d:89:de:d6:ea:41:da
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$


yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140095257118016:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69
:fopen('./demoCA/private/cakey.pem','r')
140095257118016:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (Au)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (AU)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -c
ert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_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: May 13 12:44:27 2022 GMT
Not After : May 13 12:44:27 2023 GMT
Subject:
countryName = AU
stateOrProvinceName = QLD
organizationName = securitylab
commonName = Yasin Cakar
emailAddress = yasin.c@sigmasecurity.com.au
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
31:2C:D4:BF:1D:53:A2:DF:C0:05:A2:AE:52:F0:84:6C:CB:74:E9:1E
X509v3 Authority Key Identifier:
keyid:64:1A:05:8B:14:B3:E9:49:B5:18:C3:F3:7D:84:A1:C9:4F:1A:25:F0
Certificate is to be certified until May 13 12:44:27 2023 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
Data Base Updated
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
3d:ed:1c:4b:d7:76:a9:f7:c9:4e:de:1b:fd:2d:d0:
53:d2:a4:90:fb:a6:94:29:1a:25:16:9c:d5:2b:74:
a1:87:b4:3e:23:60:89:d9:f7:69:16:d3:ed:47:22:
71:47:ec:16:27:8e:75:80:f5:cb:69:a6:0a:ed:11:
9b:e3:29:84:52:c7:c6:35:96:d0:03:d5:43:0d:79:
25:81
prime1:
00:d5:94:20:dc:63:08:4f:c8:92:f9:bf:d1:f7:da:
5a:3c:03:53:ed:f2:e0:2d:34:33:b7:f8:75:d9:64:
e3:21:ce:35:58:5d:87:64:78:0a:69:43:1e:db:08:
f0:bb:3b:9c:f6:80:cb:9e:af:da:60:26:be:bb:ab:
f6:f9:69:47:85:38:89:5e:bf:4a:4a:35:7d:af:8b:
63:0f:e3:20:86:1e:b5:bc:9e:7d:28:e2:e8:70:8d:
91:56:85:c9:34:47:5e:43:b7:bc:7a:8c:cd:fe:2b:
ec:68:f4:ad:86:2e:09:3e:ff:8c:4a:b5:bc:b5:c9:
21:46:f9:e4:84:d2:d1:38:65
prime2:
00:cc:af:83:82:a5:40:d6:8e:69:a2:7f:fd:a6:35:
ed:39:a7:55:ae:be:3c:e5:90:da:ad:11:a5:93:60:
d1:31:f9:a8:13:2c:e0:23:48:04:dd:ee:23:a8:c4:
be:fc:80:0a:e7:77:3b:4e:df:bf:df:53:fe:04:27:
72:8c:31:ff:03:a6:70:b8:ea:dc:f1:d3:7b:a9:fc:
27:fc:53:ec:bf:eb:b8:c6:6e:26:e1:d5:9e:6f:c0:
e0:35:5e:98:f4:fb:29:a4:2c:23:8c:92:2b:59:bc:
e3:9c:b8:c2:c3:12:92:d6:2a:23:83:92:ed:87:1c:
a0:c6:10:78:1e:ad:94:8b:d1
exponent1:
61:bc:05:45:94:b3:ea:fe:97:f3:5d:ca:11:a7:83:
ff:4e:6e:8b:c6:c6:bb:28:d6:39:eb:a2:d2:36:8e:
91:9b:b1:61:9c:7b:26:88:a0:0b:07:42:09:6d:8f:
eb:be:1d:d7:d7:9c:56:23:96:c4:c5:36:26:df:4c:
87:59:9b:f6:e4:a6:48:0b:35:4d:bc:28:a5:ba:1d:
3c:d9:ec:ba:33:37:6a:f7:03:c3:40:02:a9:ee:be:
81:5f:7b:71:46:ef:66:01:a0:68:5c:22:af:9b:1d:
f5:f1:71:ae:a3:46:6b:e3:b9:29:3e:fc:fa:1a:ed:
f5:72:c9:15:d6:fb:12:d9
exponent2:
0e:11:21:e0:a0:aa:cc:14:0d:7e:75:7d:61:26:e3:
9e:ca:b9:40:c1:22:3e:44:ae:42:a6:ab:d2:6d:1c:
f3:6a:4c:fa:c4:62:c3:09:f8:0b:a8:8a:1a:d7:2a:
a8:ff:c3:c0:14:99:a6:da:09:bd:b7:70:05:a9:10:
5e:42:31:5c:76:db:d8:59:8b:c5:b2:db:14:db:97:
83:e7:e0:a5:6f:f5:ca:ed:57:0e:be:37:9d:46:8c:
22:1e:d6:34:3f:ee:a4:b1:c3:df:ad:4b:fd:66:d5:
dd:b7:74:eb:23:23:a4:44:51:1c:81:c4:81:3c:9e:
6f:fe:41:c3:19:fa:d3:81
coefficient:
6e:e0:22:62:93:13:0f:e5:04:78:f2:53:d8:7d:2b:
ad:d1:1c:7b:60:b8:6a:27:c8:ee:9e:76:42:15:66:
68:e3:d6:f9:f5:4d:b0:4b:ec:89:67:42:ea:eb:56:
12:b9:96:ea:55:97:79:a8:32:84:16:5e:d5:78:fd:
73:06:ce:cd:98:6f:79:ab:3d:b5:35:98:0b:d2:2b:
22:d5:6c:db:36:fa:8d:9d:ca:40:14:75:20:e5:78:
2e:04:fe:5a:9f:7c:2a:f8:82:da:0c:4b:a7:6c:f5:
2b:0a:27:87:15:6c:7d:62:21:10:68:94:6a:f3:05:
11:8d:89:de:d6:ea:41:da
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$

```
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
140200635241792:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('./demoCA/private/cakey.pem','r')
140200635241792:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert /-keyfile ca.key -config myCA_openssl.cnf
Using configuration from /usr/lib/ssl/openssl.cnf
Can't open ./demoCA/private/cakey.pem for reading, No such file or directory
140095257118016:error:02001002:system library:fopen:No such file or directory:../crypto/bio/bss_file.c:69:fopen('./demoCA/private/cakey.pem','r')
140095257118016:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:76:
unable to load CA private key
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (Au)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
The countryName field is different between
CA certificate (US) and the request (AU)
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl ca -in server.csr -out server.cert -cert ca.cert -keyfile ca.key -config myCA_openssl.cnf
Using configuration from myCA_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: May 13 12:44:27 2022 GMT
            Not After : May 13 12:44:27 2023 GMT
        Subject:
            countryName               = AU
            stateOrProvinceName       = QLD
            organizationName          = securitylab
            commonName                = Yasin Cakar
            emailAddress              = yasin.c@sigmasecurity.com.au
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                31:2C:D4:BF:1D:53:A2:DF:C0:05:A2:AE:52:F0:84:6C:CB:74:E9:1E
            X509v3 Authority Key Identifier:
                keyid:64:1A:05:8B:14:B3:E9:49:B5:18:C3:F3:7D:84:A1:C9:4F:1A:25:F0

Certificate is to be certified until May 13 12:44:27 2023 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
Data Base Updated
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$
```



Step 3. Configuring a web server for securitylab2022.com.

1. Configuring a DNS. Open and edit /etc/hosts

   ```
   $ sudo gedit /etc/hosts
   ```

   and add the following line

   ```
   127.0.0.1 securitylab2022.com
   ```

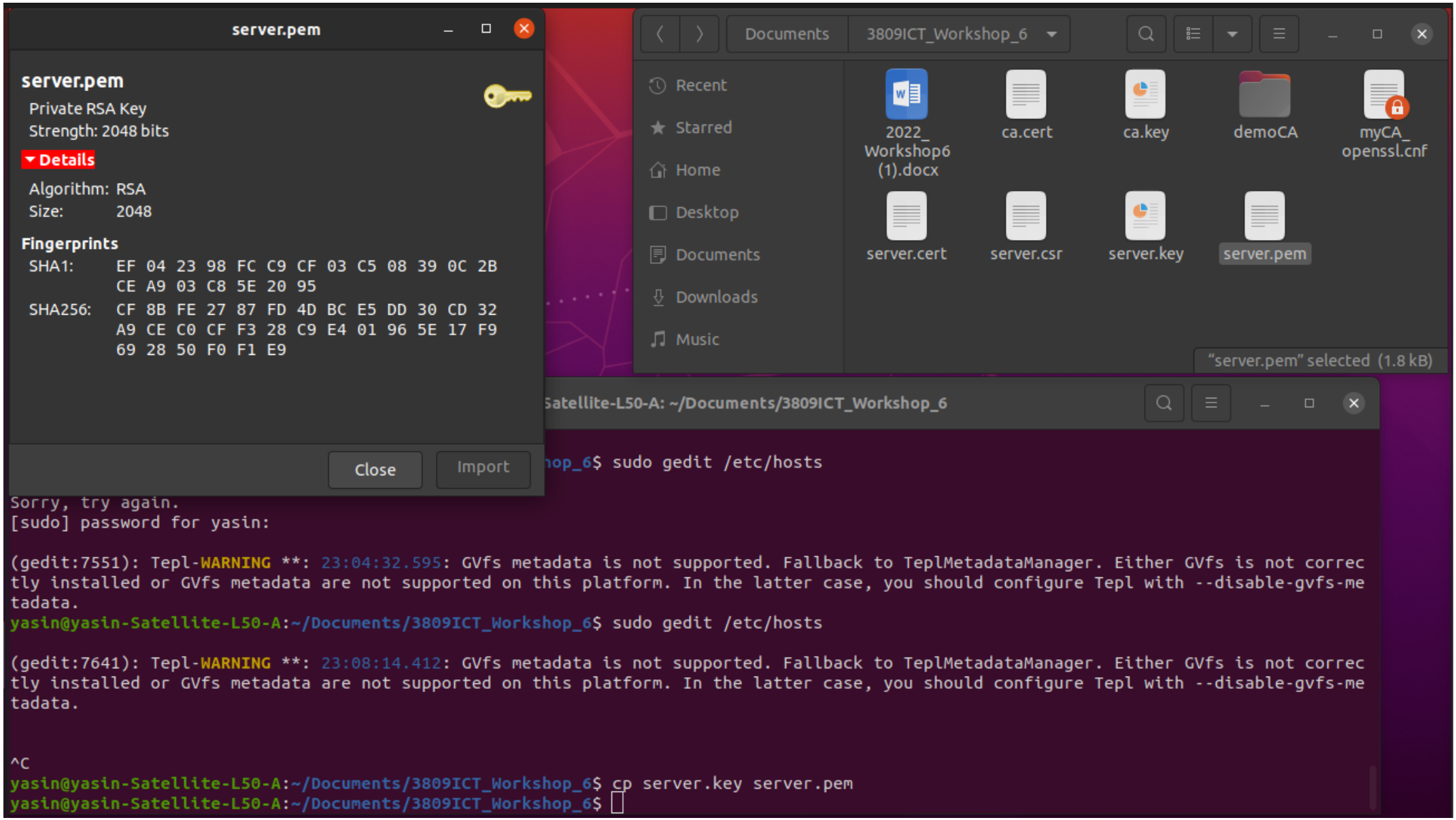
   (Since we are doing experiment locally, we use address 127.0.0.1 and map securitylab2022.com to it.)

2. Combine the private key and (public) certificate into a single file.

   ```
   $ cp server.key server.pem
   # Copying the sever private key into server.pem
   ```

   $ cat server.cert >> server.pem

   Answer:

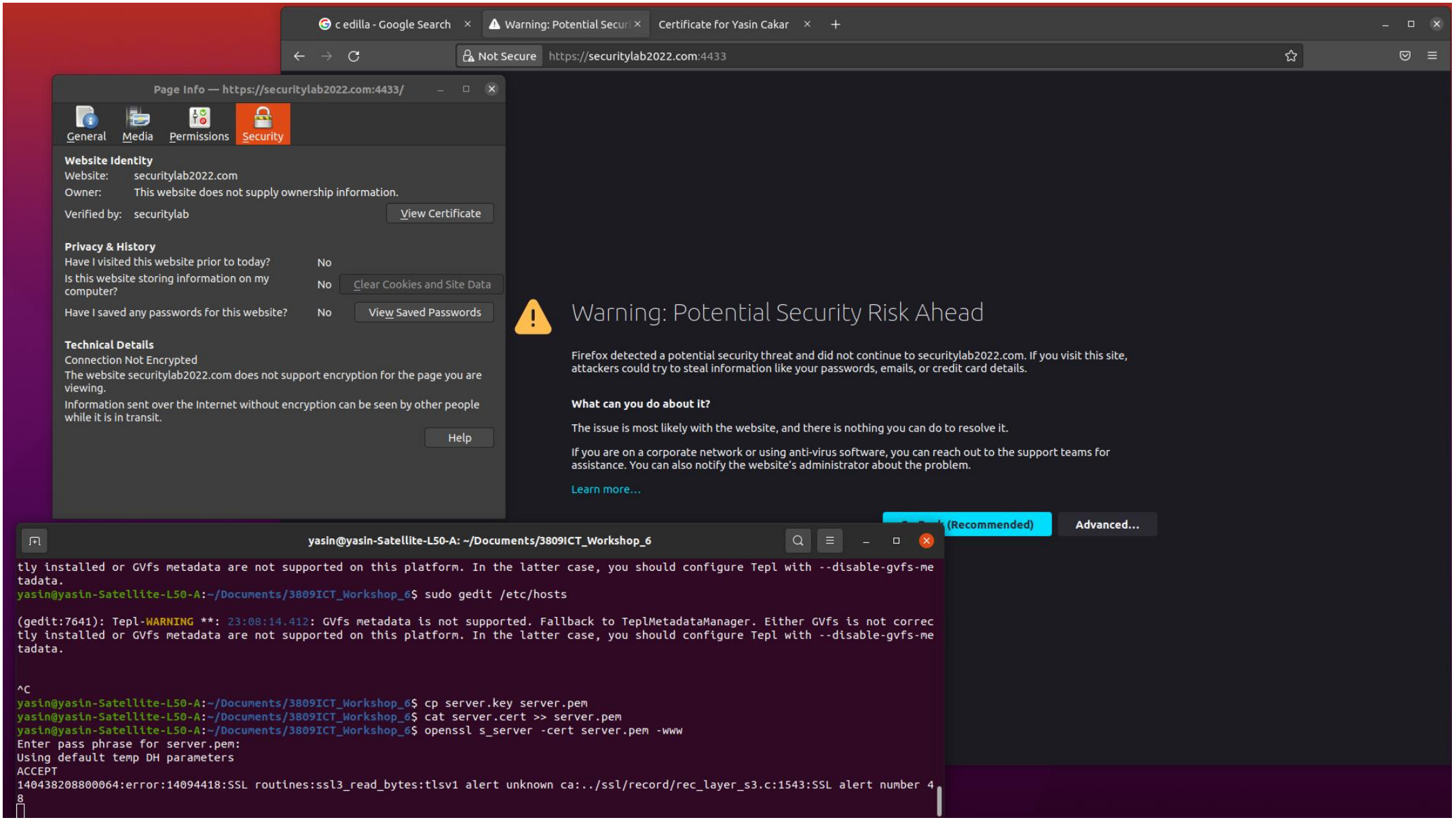

server.pem
server.pem
Private RSA Key
Strength: 2048 bits
Details
Algorithm: RSA
Size: 2048
Fingerprints
SHA1: EF 04 23 98 FC C9 CF 03 C5 08 39 0C 2B CE A9 03 C8 5E 20 95
SHA256: CF 8B FE 27 87 FD 4D BC E5 DD 30 CD 32 A9 CE C0 CF F3 28 C9 E4 01 96 5E 17 F9 69 28 50 F0 F1 E9
Close
Import
Documents
3809ICT_Workshop_6
Recent
Starred
Home
Desktop
Documents
Downloads
Music
2022_ Workshop6 (1).docx
ca.cert
ca.key
demoCA
myCA_ openssl.cnf
server.cert
server.csr
server.key
server.pem
"server.pem" selected (1.8 kB)
Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
op_6$ sudo gedit /etc/hosts
Sorry, try again.
[sudo] password for yasin:
(gedit:7551): Tepl-WARNING **: 23:04:32.595: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ sudo gedit /etc/hosts
(gedit:7641): Tepl-WARNING **: 23:08:14.412: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-metadata.
^C
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ cp server.key server.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$

3. Launch the web server using server.pem (pass phrase for server.pem, i.e., server.key is needed)

   ```
   $ openssl s_server -cert server.pem -www
   ```

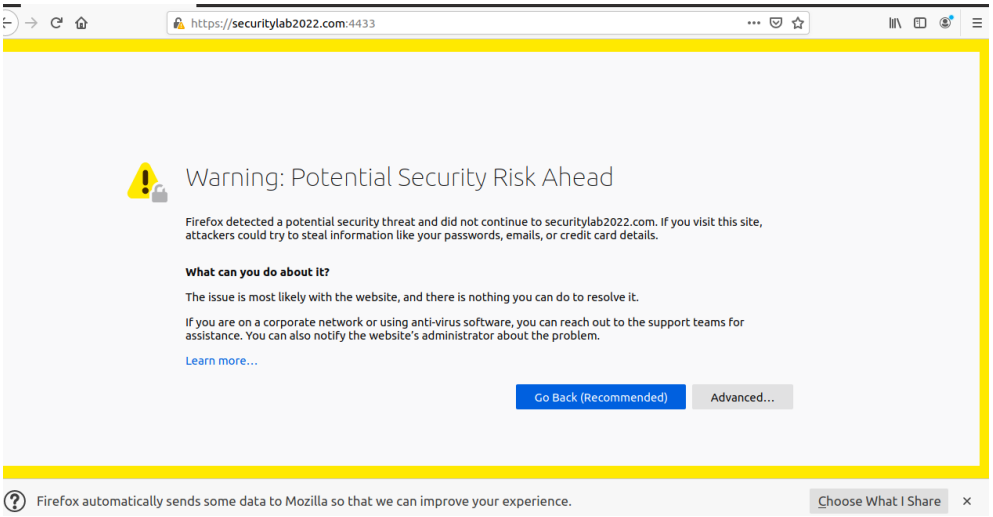
   Now, the server is listening on port 4433.

   Answer:

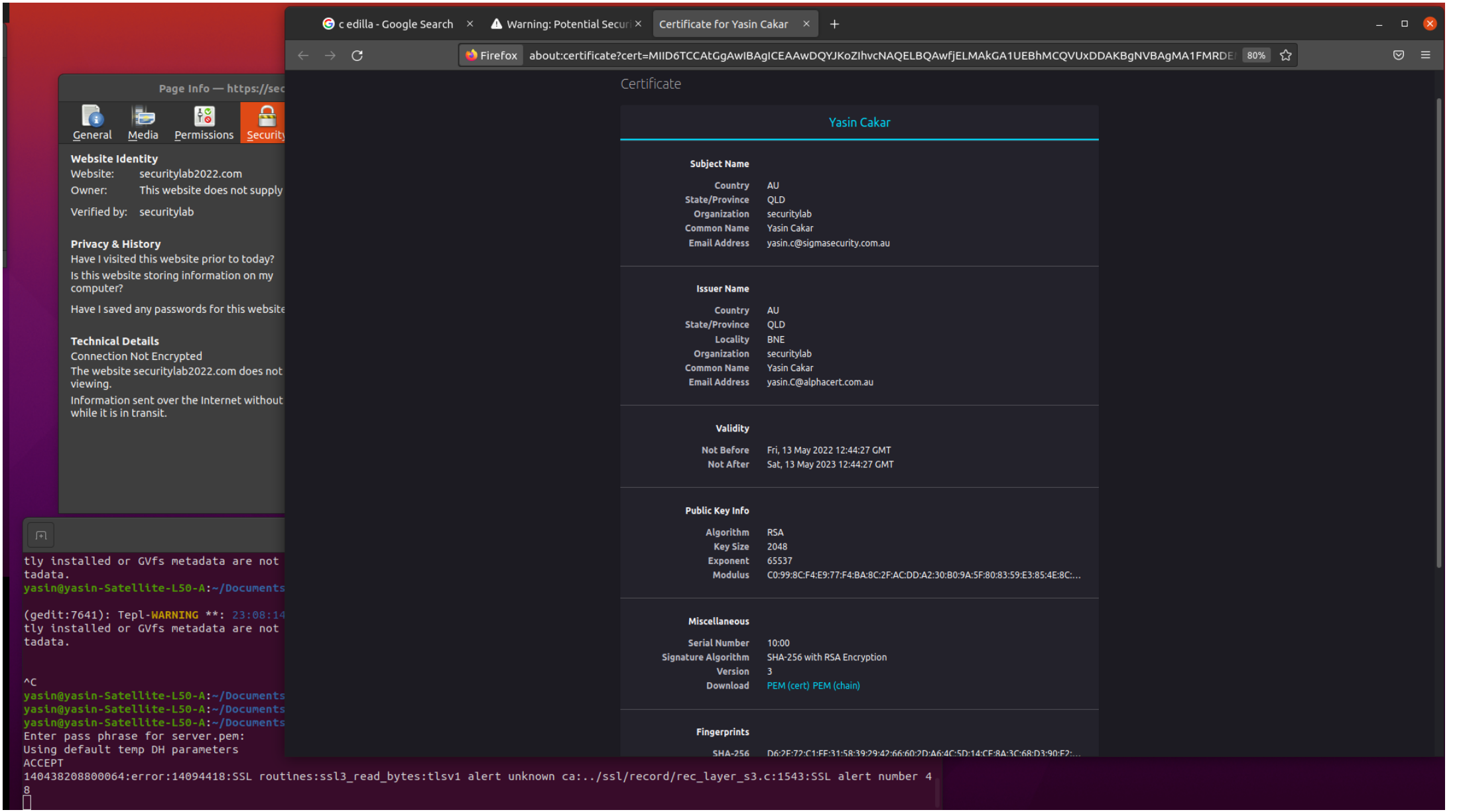

c edilla - Google Search
Warning: Potential Securi
Certificate for Yasin Cakar
Not Secure
https://securitylab2022.com:4433
Page Info — https://securitylab2022.com:4433/
General
Media
Permissions
Security
Website Identity
Website: securitylab2022.com
Owner: This website does not supply ownership information.
Verified by: securitylab
View Certificate
Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? No
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Not Encrypted
The website securitylab2022.com does not support encryption for the page you are viewing.
Information sent over the Internet without encryption can be seen by other people while it is in transit.
Help
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to securitylab2022.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it.
If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.
Learn more...
(Recommended)
Advanced...
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
tly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-me
tadata.
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ sudo gedit /etc/hosts
(gedit:7641): Tepl-WARNING **: 23:08:14.412: GVfs metadata is not supported. Fallback to TeplMetadataManager. Either GVfs is not correc
tly installed or GVfs metadata are not supported on this platform. In the latter case, you should configure Tepl with --disable-gvfs-me
tadata.
^C
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ cp server.key server.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ cat server.cert >> server.pem
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
140438208800064:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:../ssl/record/rec_layer_s3.c:1543:SSL alert number 4
8

4. Let's open application Wireshark, select the interface "Loopback: lo" and start listening. In this step, we basically wanted to see how TLS handshake packets. Open your web browser and go to https://securitylab2022.com:4433/.

   You will see a warning information as below



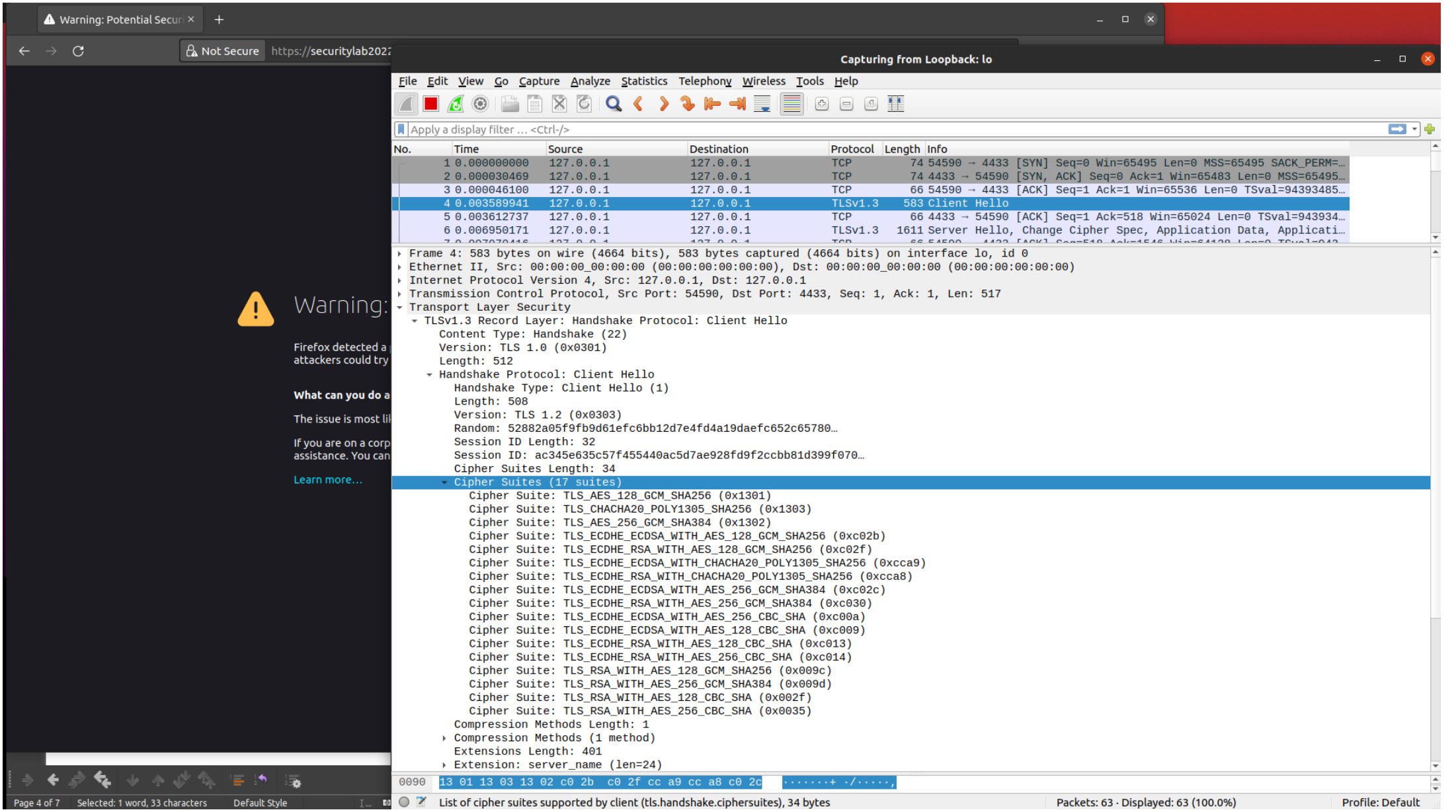
Answer:


c edilla - Google Search
Warning: Potential Securi
Certificate for Yasin Cakar
Firefox
about:certificate?cert=MIID6TCCAtGgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwfjELMAkGA1UEBhMCQVUxDDAKBgNVBAgMA1FMRDE
80%
Page Info — https://sec
General
Media
Permissions
Security
Website Identity
Website: securitylab2022.com
Owner: This website does not supply
Verified by: securitylab
Privacy & History
Have I visited this website prior to today?
Is this website storing information on my computer?
Have I saved any passwords for this website
Technical Details
Connection Not Encrypted
The website securitylab2022.com does not
viewing.
Information sent over the Internet without
while it is in transit.
Certificate
Yasin Cakar
Subject Name
Country AU
State/Province QLD
Organization securitylab
Common Name Yasin Cakar
Email Address yasin.c@sigmasecurity.com.au
Issuer Name
Country AU
State/Province QLD
Locality BNE
Organization securitylab
Common Name Yasin Cakar
Email Address yasin.C@alphacert.com.au
Validity
Not Before Fri, 13 May 2022 12:44:27 GMT
Not After Sat, 13 May 2023 12:44:27 GMT
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus C0:99:8C:F4:E9:77:F4:BA:8C:2F:AC:DD:A2:30:B0:9A:5F:80:83:59:E3:85:4E:8C:...
Miscellaneous
Serial Number 10:00
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256
tly installed or GVfs metadata are not
tadata.
yasin@yasin-Satellite-L50-A:~/Documents
(gedit:7641): Tepl-WARNING **: 23:08:14
tly installed or GVfs metadata are not
tadata.
^C
yasin@yasin-Satellite-L50-A:~/Documents
yasin@yasin-Satellite-L50-A:~/Documents
yasin@yasin-Satellite-L50-A:~/Documents
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
140438208800064:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:../ssl/record/rec_layer_s3.c:1543:SSL alert number 4
8

Q: Identify the Client Hello packet. What are the Cipher Suites supported by your web browser? (Take a screenshot.)

Answer:

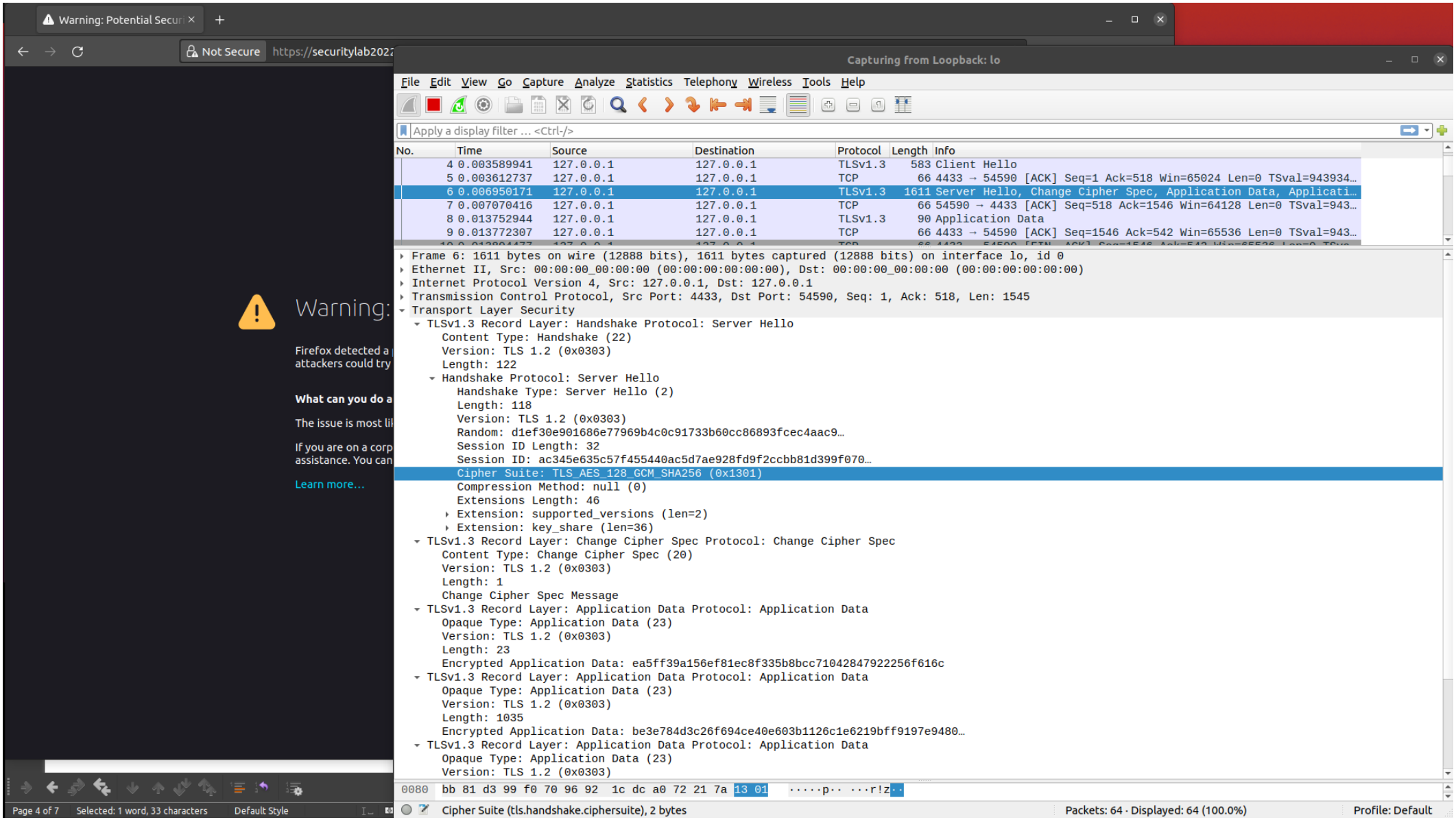
Session ID Length: 32
Session ID: ac345e635c57f455440ac5d7ae928fd9f2ccbb81d399f070…
Cipher Suites Length: 34
Cipher Suites (17 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) *
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1


Warning: Potential Secur
Not Secure
https://securitylab202
Warning:
Firefox detected a
attackers could try
What can you do a
The issue is most li
If you are on a corp
assistance. You can
Learn more...
Page 4 of 7
Selected: 1 word, 33 characters
Default Style
Capturing from Loopback: lo
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 127.0.0.1 127.0.0.1 TCP 74 54590 → 4433 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=…
2 0.000030469 127.0.0.1 127.0.0.1 TCP 74 4433 → 54590 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495…
3 0.000046100 127.0.0.1 127.0.0.1 TCP 66 54590 → 4433 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=94393485…
4 0.003589941 127.0.0.1 127.0.0.1 TLSv1.3 583 Client Hello
5 0.003612737 127.0.0.1 127.0.0.1 TCP 66 4433 → 54590 [ACK] Seq=1 Ack=518 Win=65024 Len=0 TSval=943934…
6 0.006950171 127.0.0.1 127.0.0.1 TLSv1.3 1611 Server Hello, Change Cipher Spec, Application Data, Applicati…
Frame 4: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface lo, id 0
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 54590, Dst Port: 4433, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 52882a05f9fb9d61efc6bb12d7e4fd4a19daefc652c65780…
Session ID Length: 32
Session ID: ac345e635c57f455440ac5d7ae928fd9f2ccbb81d399f070…
Cipher Suites Length: 34
Cipher Suites (17 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 401
Extension: server_name (len=24)
0090 13 01 13 03 13 02 c0 2b c0 2f cc a9 cc a8 c0 2c
List of cipher suites supported by client (tls.handshake.ciphersuites), 34 bytes
Packets: 63 · Displayed: 63 (100.0%)
Profile: Default

Q: Identify the Server Hello packet. What is the Cipher Suit chosen by the server? And what (Take screenshots.) Where is the server's certificate? (Hint: see the field "Key Share Extension" for both Client Hello and Server Hello and think what they are.)

Answer:

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)



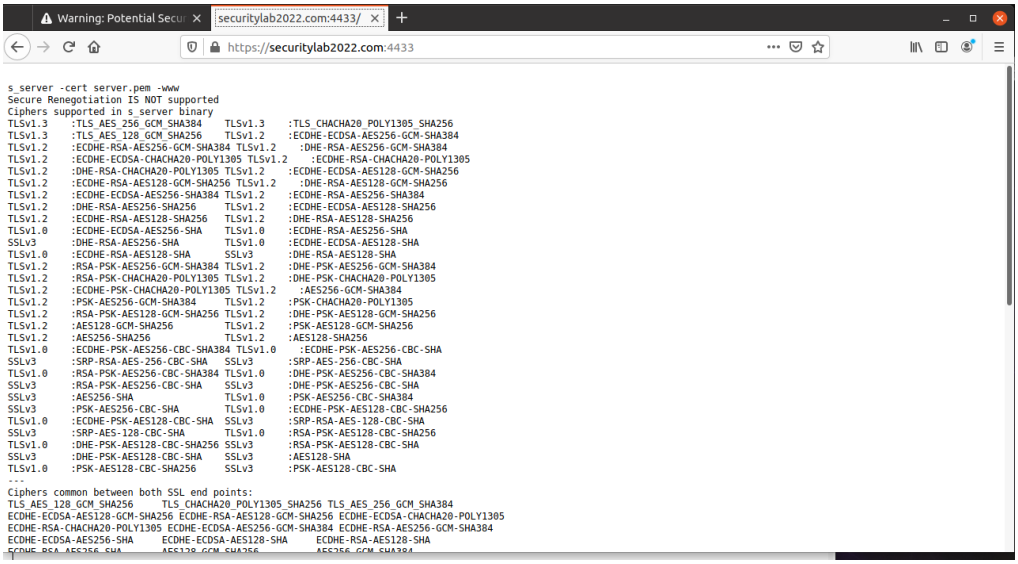
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Q: Why does this warning information appeared? Click on the little lock icon on the URL bar before the URL and go to “More Information” and then “View Certificate”. Think about what has been missing and confirm your thought.

Answer:
The web browser cannot verify our certificate as we are an unknown certificate authority, as we just created the certificate. This is why a warning information appears on the webpage.

For the browser to verify our certificate we need to upload the CA’s certificate we just created.

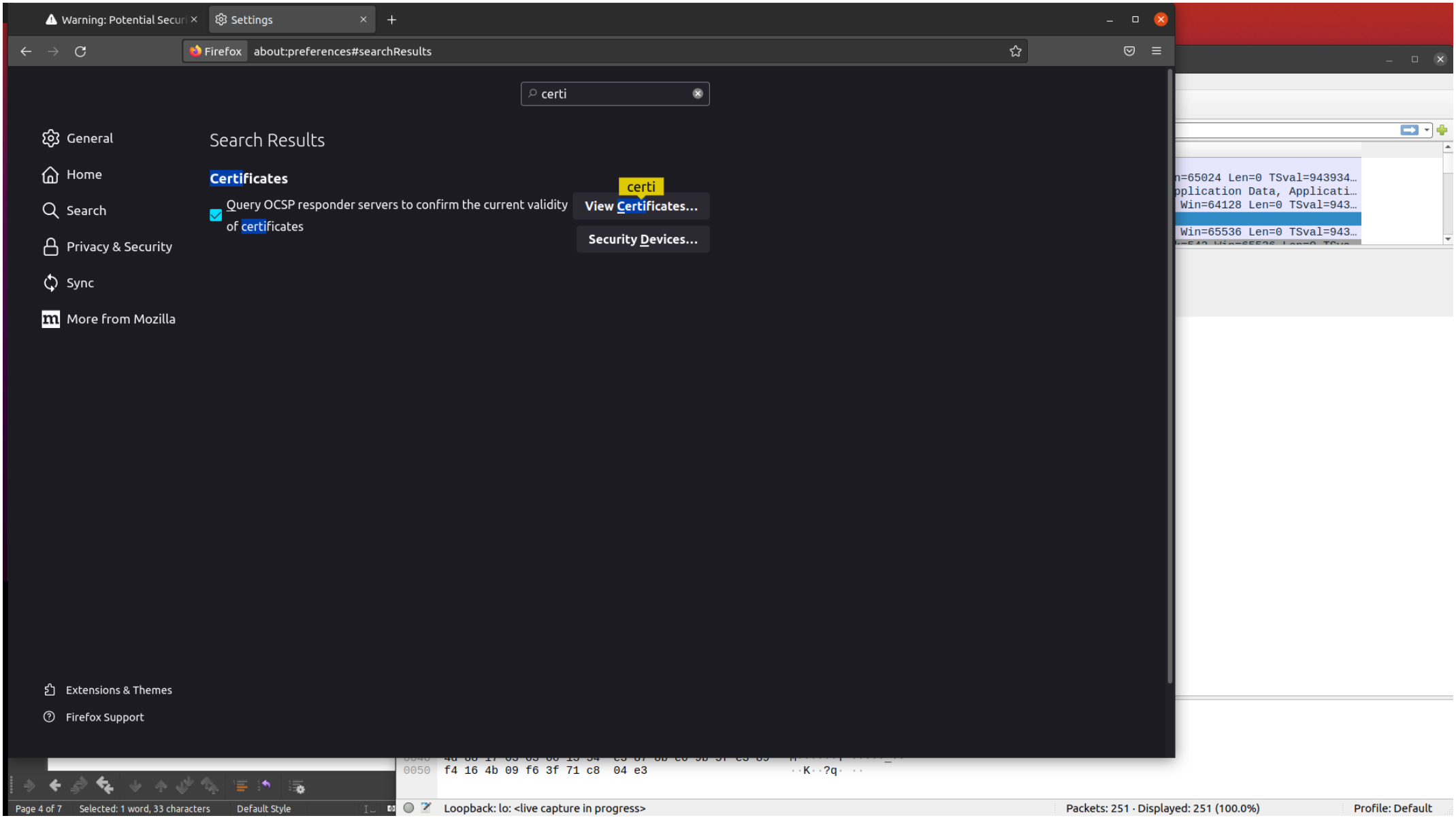
5. Uploading CA’s certificate. Search for "certificate" in Firefox web browser's preferences page, click on "View Certificates" and enter "Certificate Manager", click on "Authorities tab" and import ca.cert. Check "Trust this CA to identify web sites". Then, reload https://securitylab2022.com:4433/. You will see

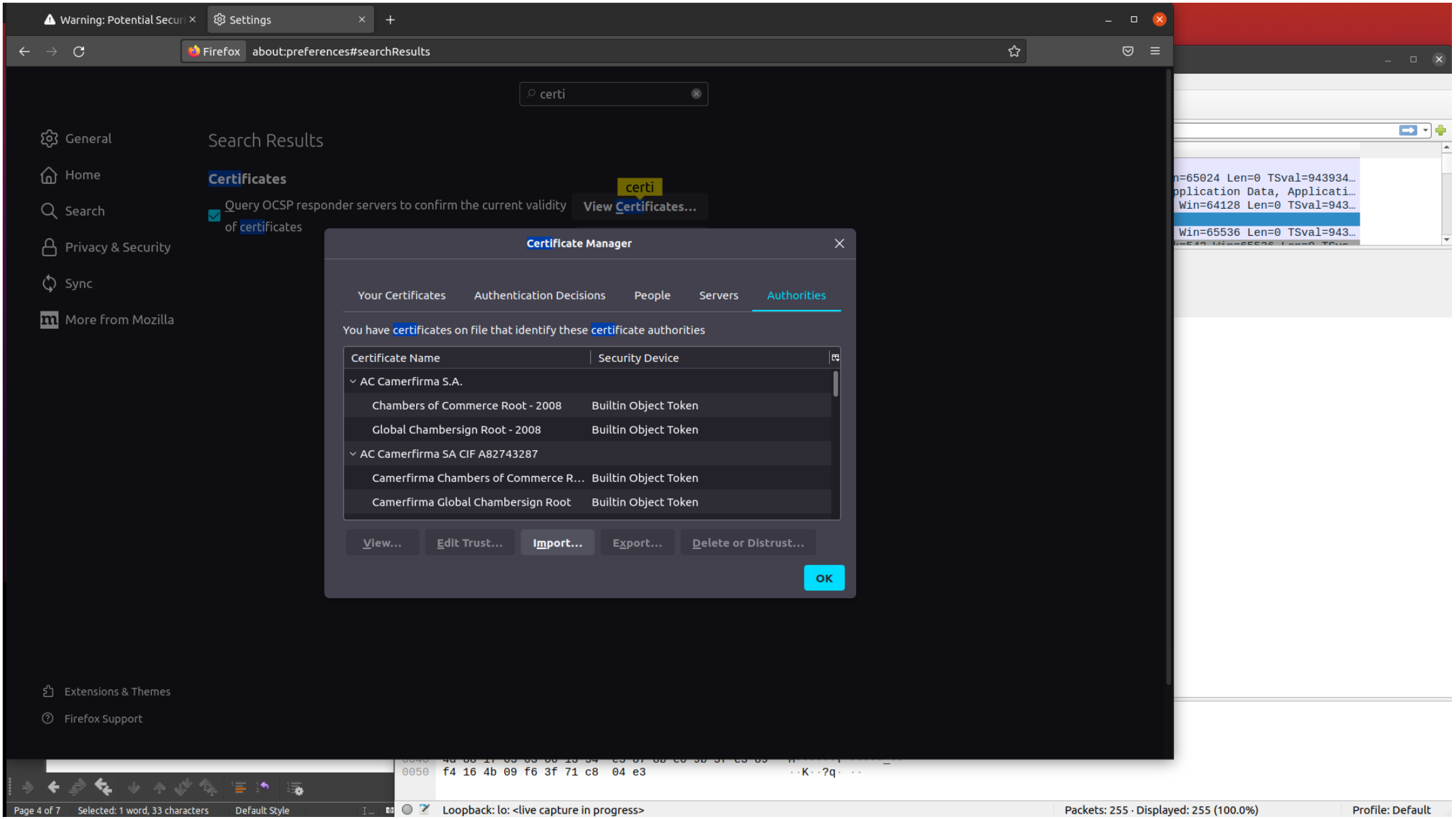


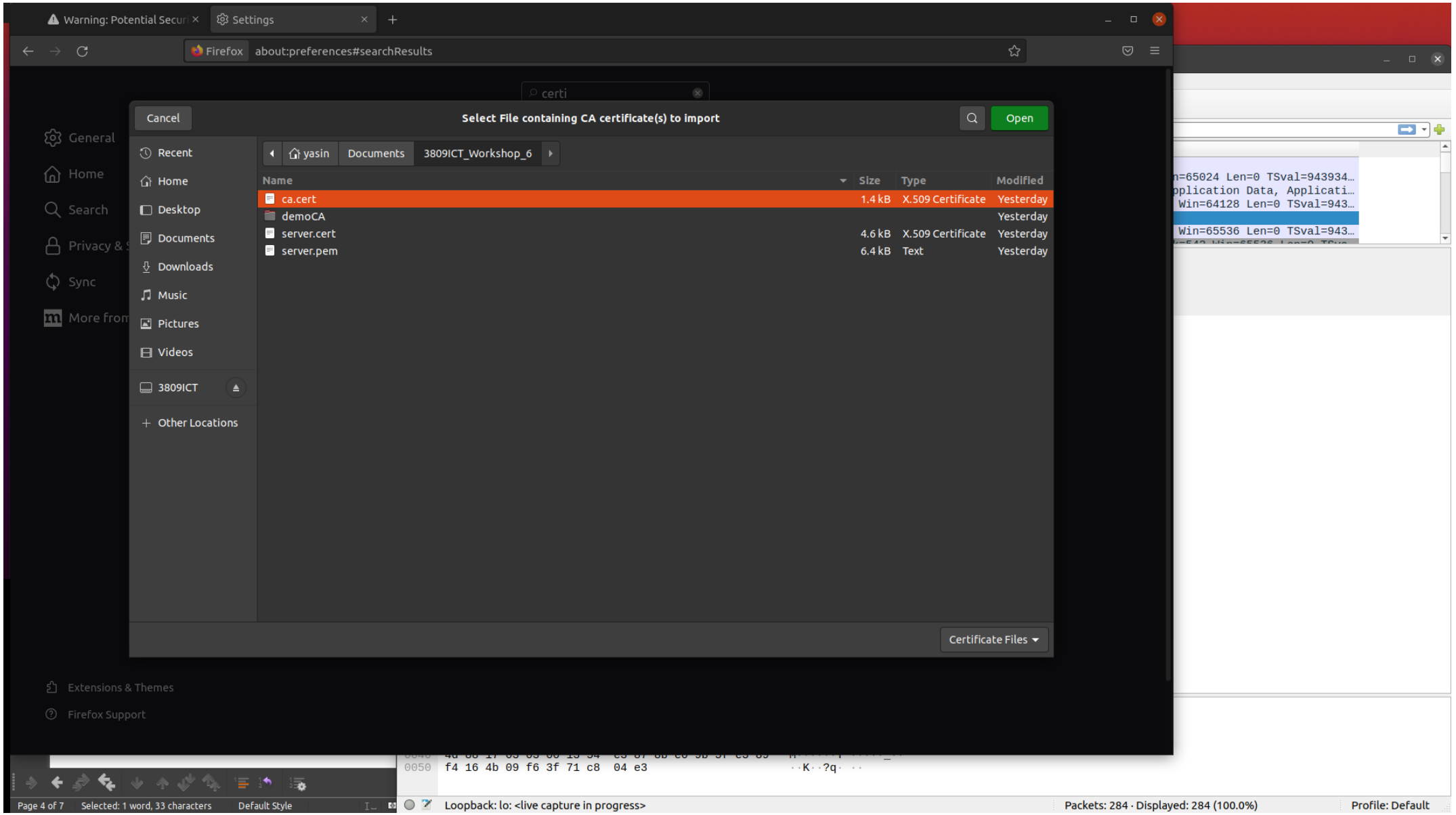
which means the certificate is verified (though you can see the certificate issuer, which is yourself is not recognized by Mozilla, the web browser producer).

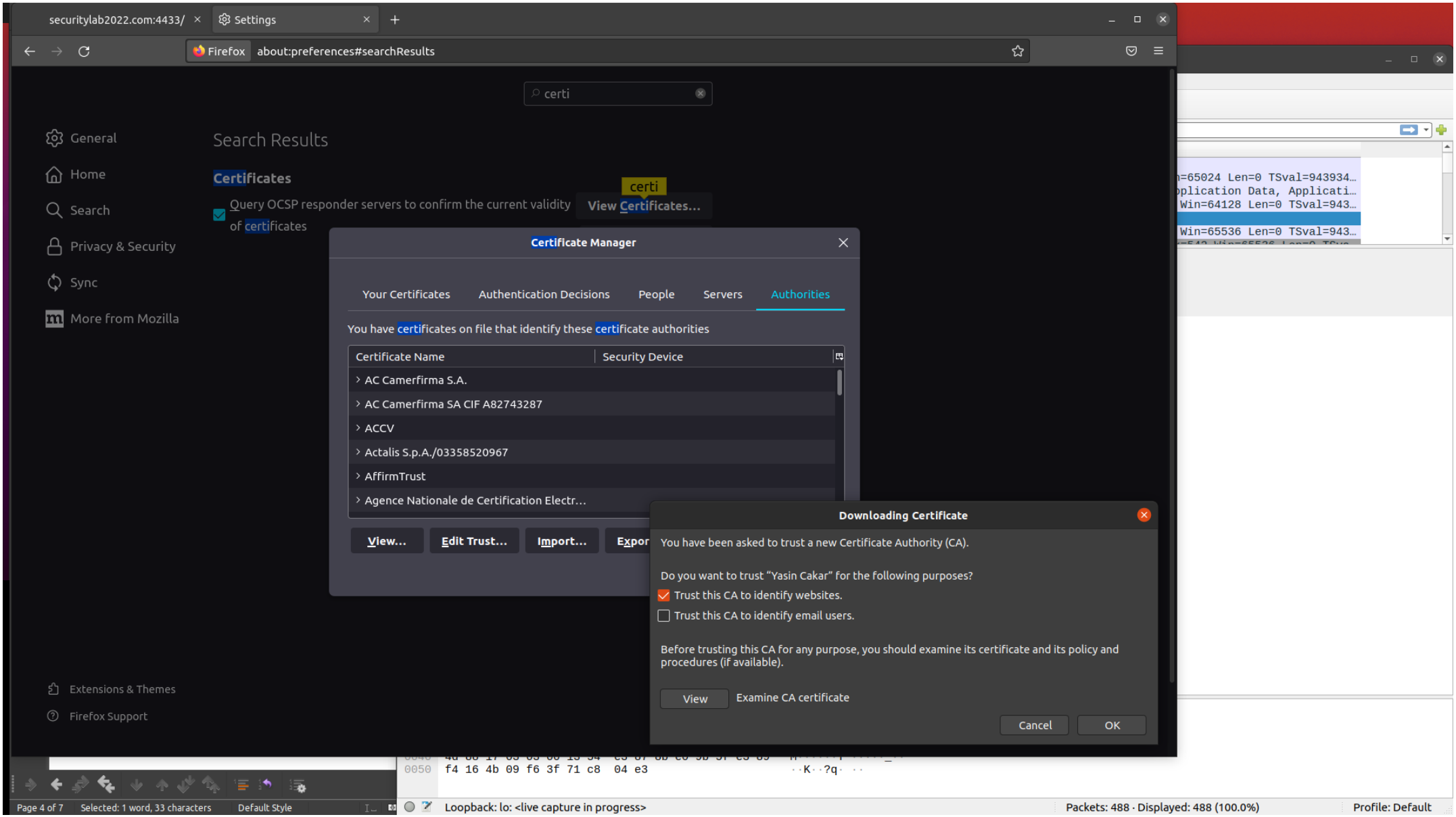
Meanwhile, at Wireshark you can see TLSv1.3 application data packets have been transmitted through, and they are encrypted and authenticated (using the symmetric-key cipher and the message authentication codes respectively negotiated during handshake phase.)

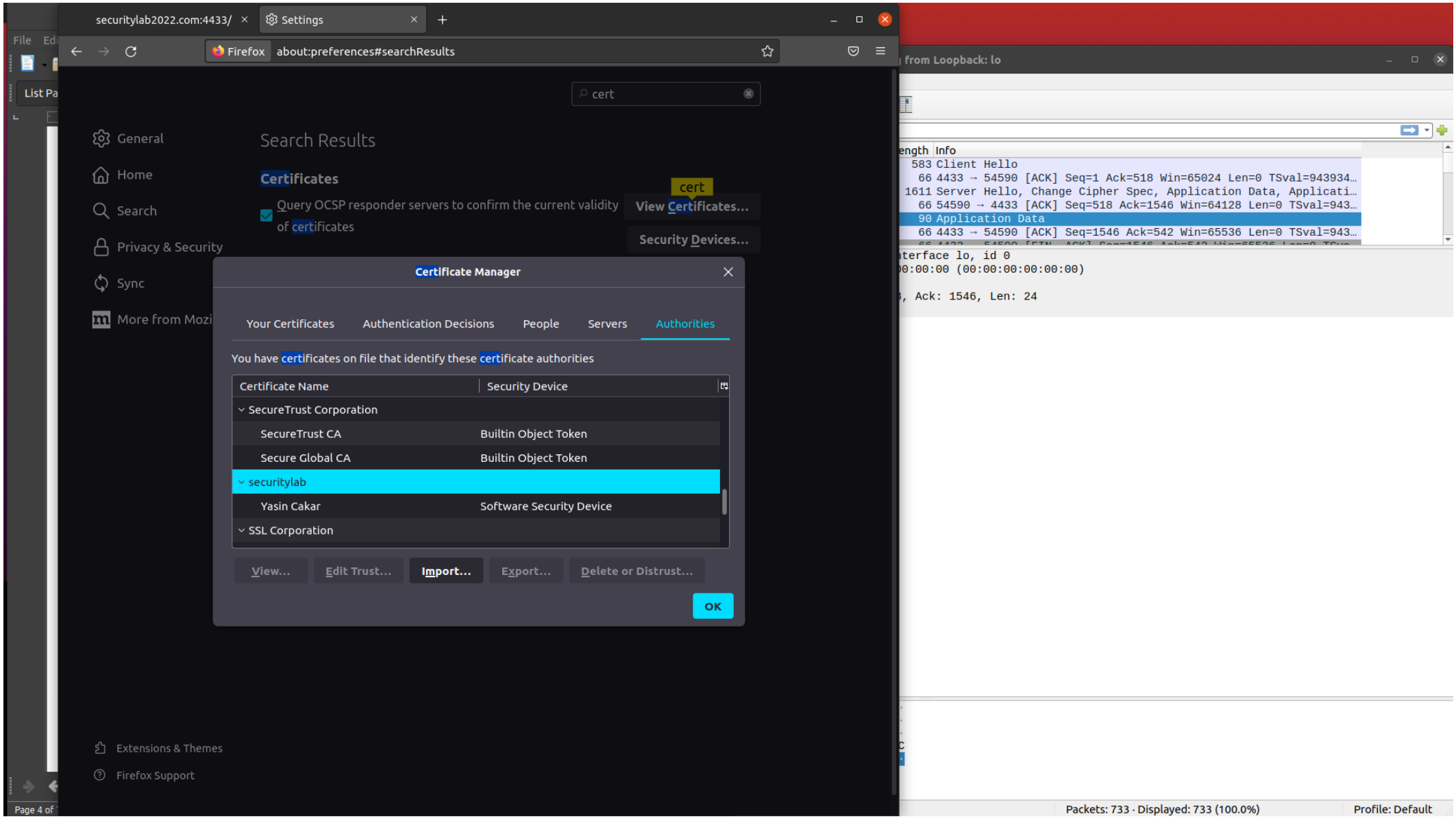
Answer:
For some reason the browser did not use my certificate to verify after uploading. The upload was successful however the padlock icon still had the “ ⚠ ” sign

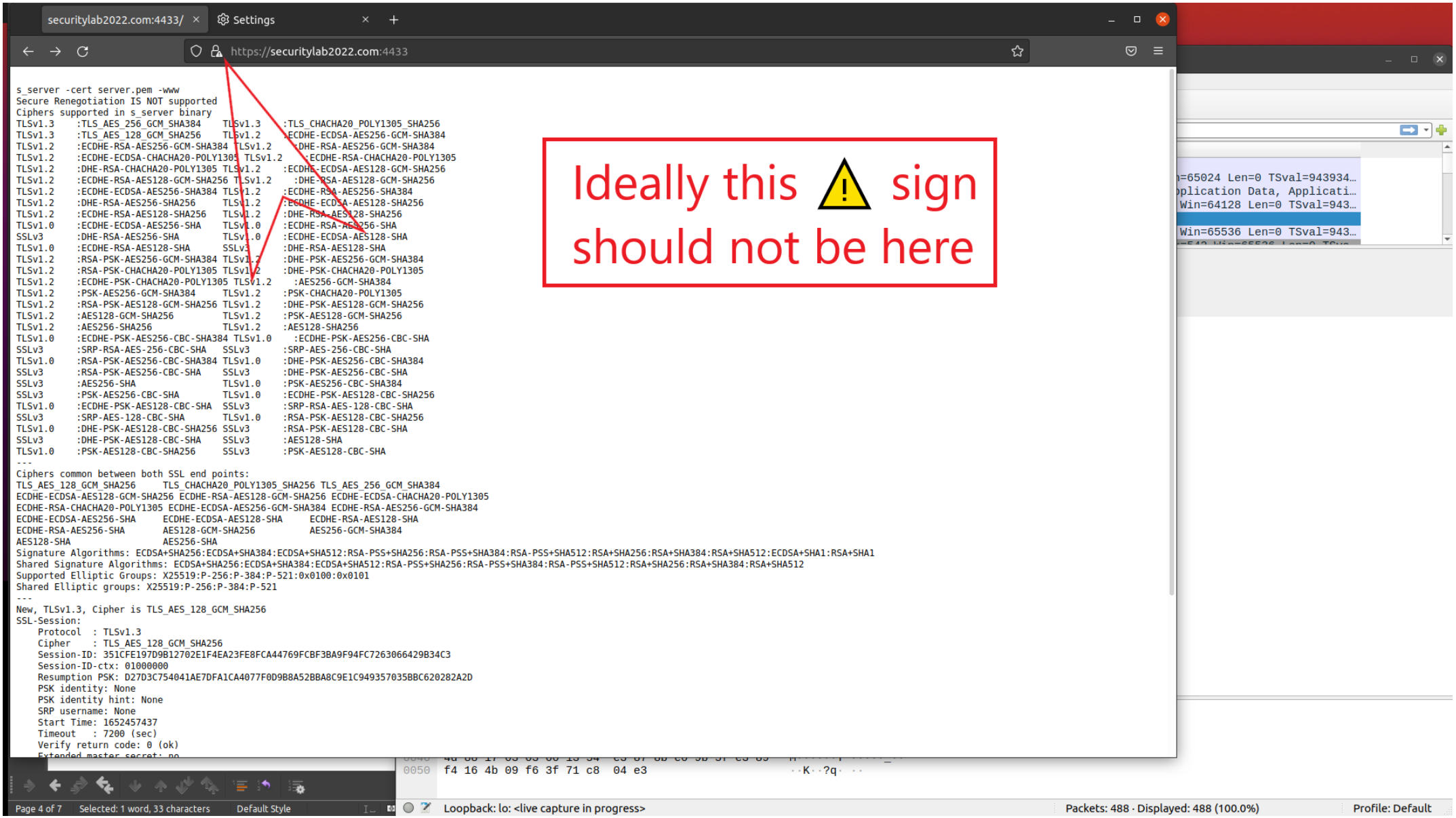

Warning: Potential Securi
Settings
Firefox
about:preferences#searchResults
certi
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Search Results
Certificates
Query OCSP responder servers to confirm the current validity of certificates
certi
View Certificates...
Security Devices...
Extensions & Themes
Firefox Support
Page 4 of 7
Selected: 1 word, 33 characters
Default Style
0050 f4 16 4b 09 f6 3f 71 c8 04 e3
Loopback: lo: <live capture in progress>
Packets: 251 · Displayed: 251 (100.0%)
Profile: Default


Warning: Potential Secur
Settings
Firefox
about:preferences#searchResults
certi
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Search Results
Certificates
Query OCSP responder servers to confirm the current validity of certificates
certi
View Certificates...
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
AC Camerfirma S.A.
Chambers of Commerce Root - 2008
Builtin Object Token
Global Chambersign Root - 2008
Builtin Object Token
AC Camerfirma SA CIF A82743287
Camerfirma Chambers of Commerce R...
Builtin Object Token
Camerfirma Global Chambersign Root
Builtin Object Token
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK
Extensions & Themes
Firefox Support
Page 4 of 7
Selected: 1 word, 33 characters
Default Style
0050 f4 16 4b 09 f6 3f 71 c8 04 e3
Loopback: lo: <live capture in progress>
Packets: 255 · Displayed: 255 (100.0%)
Profile: Default


Warning: Potential Secur
Settings
Firefox
about:preferences#searchResults
certi
General
Home
Search
Privacy &
Sync
More from
Cancel
Select File containing CA certificate(s) to import
Open
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
3809ICT
Other Locations
yasin
Documents
3809ICT_Workshop_6
Name
Size
Type
Modified
ca.cert
1.4 kB
X.509 Certificate
Yesterday
demoCA
Yesterday
server.cert
4.6 kB
X.509 Certificate
Yesterday
server.pem
6.4 kB
Text
Yesterday
Certificate Files
Extensions & Themes
Firefox Support
=65024 Len=0 TSval=943934…
pplication Data, Applicati…
Win=64128 Len=0 TSval=943…
Win=65536 Len=0 TSval=943…
0050 f4 16 4b 09 f6 3f 71 c8 04 e3
Page 4 of 7
Selected: 1 word, 33 characters
Default Style
Loopback: lo: <live capture in progress>
Packets: 284 · Displayed: 284 (100.0%)
Profile: Default


securitylab2022.com:4433/
Settings
Firefox
about:preferences#searchResults
certi
General
Home
Search
Privacy & Security
Sync
More from Mozilla
Search Results
Certificates
Query OCSP responder servers to confirm the current validity of certificates
certi
View Certificates...
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
AC Camerfirma S.A.
AC Camerfirma SA CIF A82743287
ACCV
Actalis S.p.A./03358520967
AffirmTrust
Agence Nationale de Certification Electr...
View...
Edit Trust...
Import...
Expor
Downloading Certificate
You have been asked to trust a new Certificate Authority (CA).
Do you want to trust "Yasin Cakar" for the following purposes?
Trust this CA to identify websites.
Trust this CA to identify email users.
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).
View
Examine CA certificate
Cancel
OK
Extensions & Themes
Firefox Support
Page 4 of 7
Selected: 1 word, 33 characters
Default Style
0050 f4 16 4b 09 f6 3f 71 c8 04 e3
Loopback: lo: <live capture in progress>
Packets: 488 · Displayed: 488 (100.0%)
Profile: Default


securitylab2022.com:4433/
Settings
Firefox
about:preferences#searchResults
cert
General
Home
Search
Privacy & Security
Sync
More from Mozi
Search Results
Certificates
Query OCSP responder servers to confirm the current validity of certificates
cert
View Certificates...
Security Devices...
Certificate Manager
Your Certificates
Authentication Decisions
People
Servers
Authorities
You have certificates on file that identify these certificate authorities
Certificate Name
Security Device
SecureTrust Corporation
SecureTrust CA
Builtin Object Token
Secure Global CA
Builtin Object Token
securitylab
Yasin Cakar
Software Security Device
SSL Corporation
View...
Edit Trust...
Import...
Export...
Delete or Distrust...
OK
Extensions & Themes
Firefox Support
from Loopback: lo
583 Client Hello
66 4433 → 54590 [ACK] Seq=1 Ack=518 Win=65024 Len=0 TSval=943934…
1611 Server Hello, Change Cipher Spec, Application Data, Applicati…
66 54590 → 4433 [ACK] Seq=518 Ack=1546 Win=64128 Len=0 TSval=943…
90 Application Data
66 4433 → 54590 [ACK] Seq=1546 Ack=542 Win=65536 Len=0 TSval=943…
Packets: 733 · Displayed: 733 (100.0%)
Profile: Default


securitylab2022.com:4433/
Settings
https://securitylab2022.com:4433
Ideally this ⚠ sign should not be here
s_server -cert server.pem -www
Secure Renegotiation IS NOT supported
Ciphers supported in s_server binary
TLSv1.3 :TLS_AES_256_GCM_SHA384 TLSv1.3 :TLS_CHACHA20_POLY1305_SHA256
TLSv1.3 :TLS_AES_128_GCM_SHA256 TLSv1.2 :ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1.2 :ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 :DHE-RSA-AES256-GCM-SHA384
TLSv1.2 :ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 :ECDHE-RSA-CHACHA20-POLY1305
TLSv1.2 :DHE-RSA-CHACHA20-POLY1305 TLSv1.2 :ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1.2 :ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 :DHE-RSA-AES128-GCM-SHA256
TLSv1.2 :ECDHE-ECDSA-AES256-SHA384 TLSv1.2 :ECDHE-RSA-AES256-SHA384
TLSv1.2 :DHE-RSA-AES256-SHA256 TLSv1.2 :ECDHE-ECDSA-AES128-SHA256
TLSv1.2 :ECDHE-RSA-AES128-SHA256 TLSv1.2 :DHE-RSA-AES128-SHA256
TLSv1.0 :ECDHE-ECDSA-AES256-SHA TLSv1.0 :ECDHE-RSA-AES256-SHA
SSLv3 :DHE-RSA-AES256-SHA TLSv1.0 :ECDHE-ECDSA-AES128-SHA
TLSv1.0 :ECDHE-RSA-AES128-SHA SSLv3 :DHE-RSA-AES128-SHA
TLSv1.2 :RSA-PSK-AES256-GCM-SHA384 TLSv1.2 :DHE-PSK-AES256-GCM-SHA384
TLSv1.2 :RSA-PSK-CHACHA20-POLY1305 TLSv1.2 :DHE-PSK-CHACHA20-POLY1305
TLSv1.2 :ECDHE-PSK-CHACHA20-POLY1305 TLSv1.2 :AES256-GCM-SHA384
TLSv1.2 :PSK-AES256-GCM-SHA384 TLSv1.2 :PSK-CHACHA20-POLY1305
TLSv1.2 :RSA-PSK-AES128-GCM-SHA256 TLSv1.2 :DHE-PSK-AES128-GCM-SHA256
TLSv1.2 :AES128-GCM-SHA256 TLSv1.2 :PSK-AES128-GCM-SHA256
TLSv1.2 :AES256-SHA256 TLSv1.2 :AES128-SHA256
TLSv1.0 :ECDHE-PSK-AES256-CBC-SHA384 TLSv1.0 :ECDHE-PSK-AES256-CBC-SHA
SSLv3 :SRP-RSA-AES-256-CBC-SHA SSLv3 :SRP-AES-256-CBC-SHA
TLSv1.0 :RSA-PSK-AES256-CBC-SHA384 TLSv1.0 :DHE-PSK-AES256-CBC-SHA384
SSLv3 :RSA-PSK-AES256-CBC-SHA SSLv3 :DHE-PSK-AES256-CBC-SHA
SSLv3 :AES256-SHA TLSv1.0 :PSK-AES256-CBC-SHA384
SSLv3 :PSK-AES256-CBC-SHA TLSv1.0 :ECDHE-PSK-AES128-CBC-SHA256
TLSv1.0 :ECDHE-PSK-AES128-CBC-SHA SSLv3 :SRP-RSA-AES-128-CBC-SHA
SSLv3 :SRP-AES-128-CBC-SHA TLSv1.0 :RSA-PSK-AES128-CBC-SHA256
TLSv1.0 :DHE-PSK-AES128-CBC-SHA256 SSLv3 :RSA-PSK-AES128-CBC-SHA
SSLv3 :DHE-PSK-AES128-CBC-SHA SSLv3 :AES128-SHA
TLSv1.0 :PSK-AES128-CBC-SHA256 SSLv3 :PSK-AES128-CBC-SHA

Ciphers common between both SSL end points:
TLS_AES_128_GCM_SHA256 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_256_GCM_SHA384
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA AES128-GCM-SHA256 AES256-GCM-SHA384
AES128-SHA AES256-SHA
Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512:ECDSA+SHA1:RSA+SHA1
Shared Signature Algorithms: ECDSA+SHA256:ECDSA+SHA384:ECDSA+SHA512:RSA-PSS+SHA256:RSA-PSS+SHA384:RSA-PSS+SHA512:RSA+SHA256:RSA+SHA384:RSA+SHA512
Supported Elliptic Groups: X25519:P-256:P-384:P-521:0x0100:0x0101
Shared Elliptic groups: X25519:P-256:P-384:P-521

New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_128_GCM_SHA256
Session-ID: 351CFE197D9B12702E1F4EA23FE8FCA44769FCBF3BA9F94FC7263066429B34C3
Session-ID-ctx: 01000000
Resumption PSK: D27D3C754041AE7DFA1CA4077F0D9B8A52BBA8C9E1C949357035BBC620282A2D
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1652457437
Timeout : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
0050 f4 16 4b 09 f6 3f 71 c8 04 e3
Page 4 of 7 Selected: 1 word, 33 characters Default Style
Loopback: lo: <live capture in progress>
Packets: 488 · Displayed: 488 (100.0%)
Profile: Default

Task 3: Task 3: Analysing your TLS connection to www.griffith.edu.au

Download (from https://www.wireshark.org/download.html) and install Wireshark to your own computers (if you are using University computers from computer labs, Wireshark should be installed). If you are using Linux OSs, you can do, say, `$ sudo apt install wireshark`.

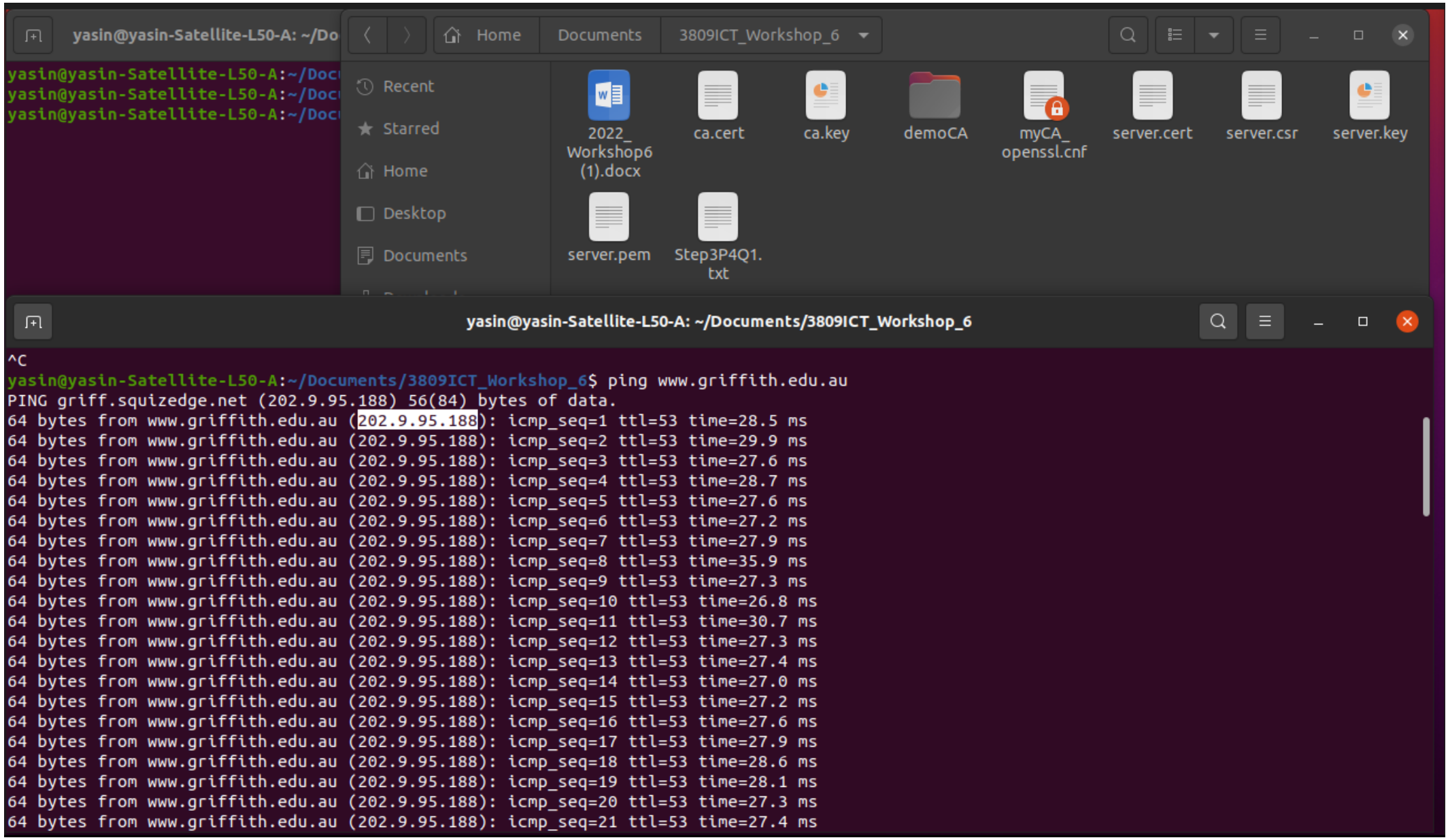
1. Open Wireshark and start listening to the network interface that connects to the Internet.
2. Open a web browser and go to www.griffith.edu.au.
3. Identify the TLS handshake packets sent between you and www.griffith.edu.au, and answer the following questions:

(To identify traffic from or two an IP address, you can go to the Wireshark filter

and type ip.addr == x where x is the address.)

Q1: What is the IP address of www.griffith.edu.au? (Hint: ping the URL)

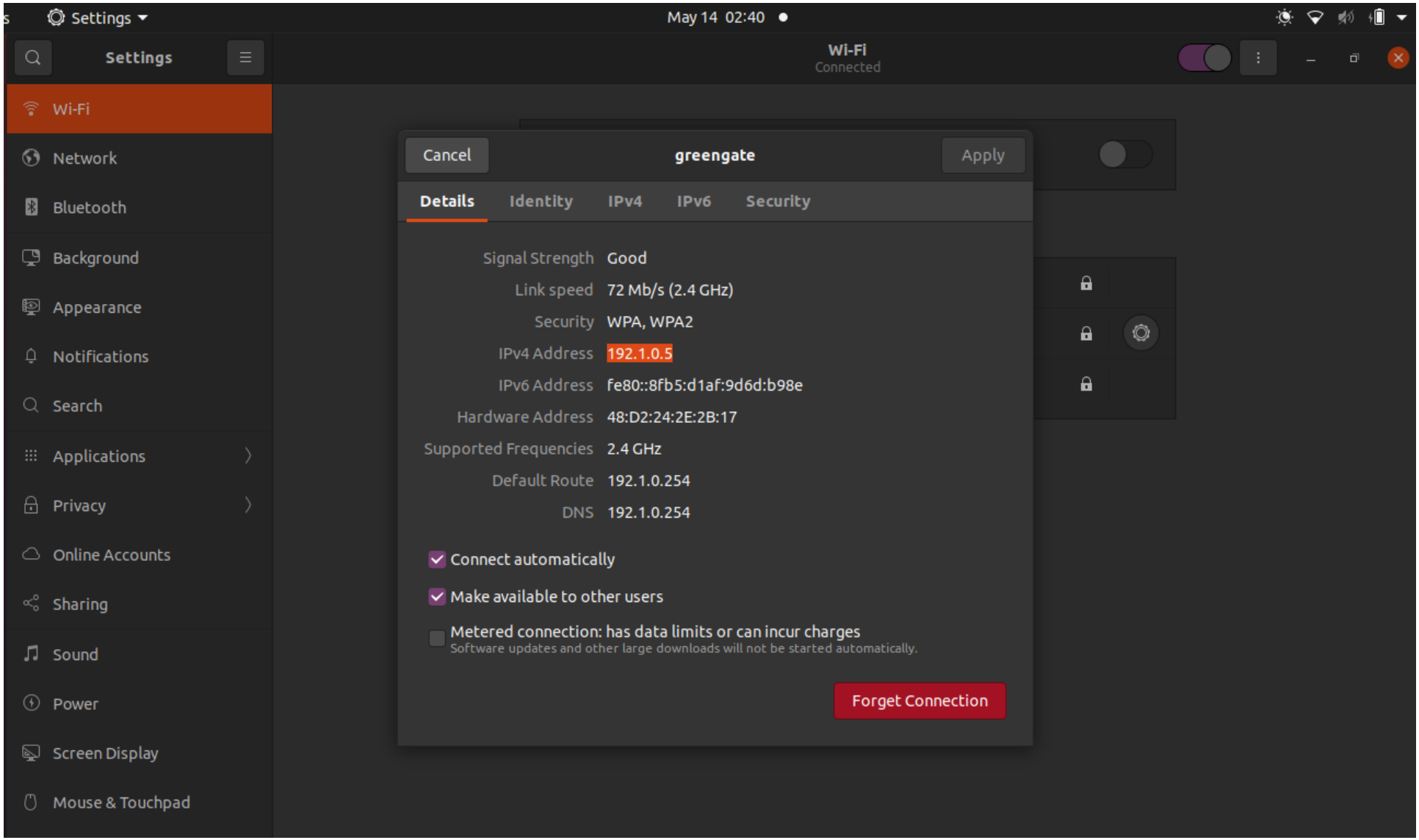
Answer:
202.9.95.188

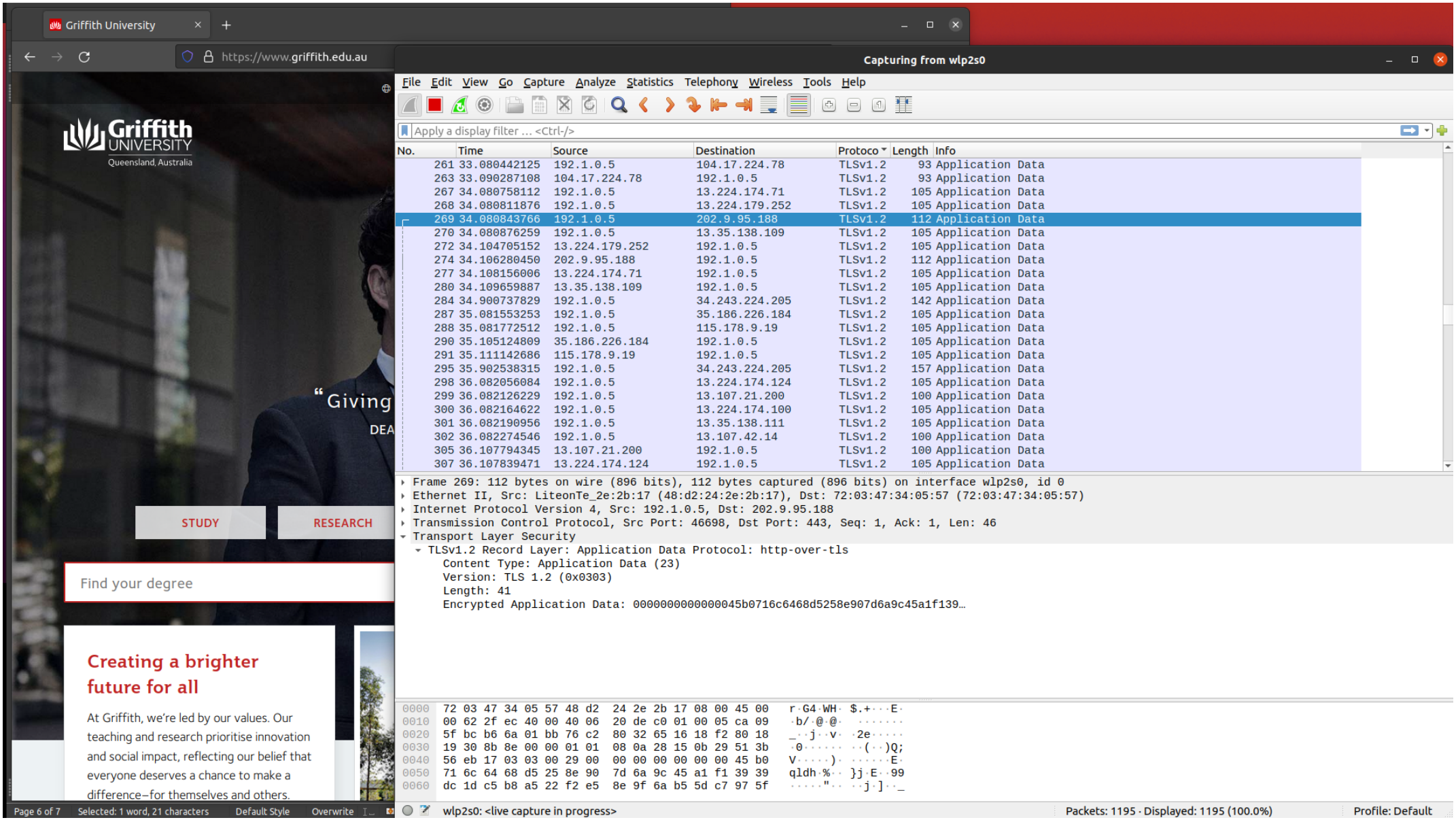

yasin@yasin-Satellite-L50-A: ~/Do
yasin@yasin-Satellite-L50-A:~/Doc
yasin@yasin-Satellite-L50-A:~/Doc
yasin@yasin-Satellite-L50-A:~/Doc
Home
Documents
3809ICT_Workshop_6
Recent
Starred
Home
Desktop
Documents
2022_ Workshop6 (1).docx
ca.cert
ca.key
demoCA
myCA_ openssl.cnf
server.cert
server.csr
server.key
server.pem
Step3P4Q1. txt
yasin@yasin-Satellite-L50-A: ~/Documents/3809ICT_Workshop_6
^C
yasin@yasin-Satellite-L50-A:~/Documents/3809ICT_Workshop_6$ ping www.griffith.edu.au
PING griff.squizedge.net (202.9.95.188) 56(84) bytes of data.
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=1 ttl=53 time=28.5 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=2 ttl=53 time=29.9 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=3 ttl=53 time=27.6 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=4 ttl=53 time=28.7 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=5 ttl=53 time=27.6 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=6 ttl=53 time=27.2 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=7 ttl=53 time=27.9 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=8 ttl=53 time=35.9 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=9 ttl=53 time=27.3 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=10 ttl=53 time=26.8 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=11 ttl=53 time=30.7 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=12 ttl=53 time=27.3 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=13 ttl=53 time=27.4 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=14 ttl=53 time=27.0 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=15 ttl=53 time=27.2 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=16 ttl=53 time=27.6 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=17 ttl=53 time=27.9 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=18 ttl=53 time=28.6 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=19 ttl=53 time=28.1 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=20 ttl=53 time=27.3 ms
64 bytes from www.griffith.edu.au (202.9.95.188): icmp_seq=21 ttl=53 time=27.4 ms

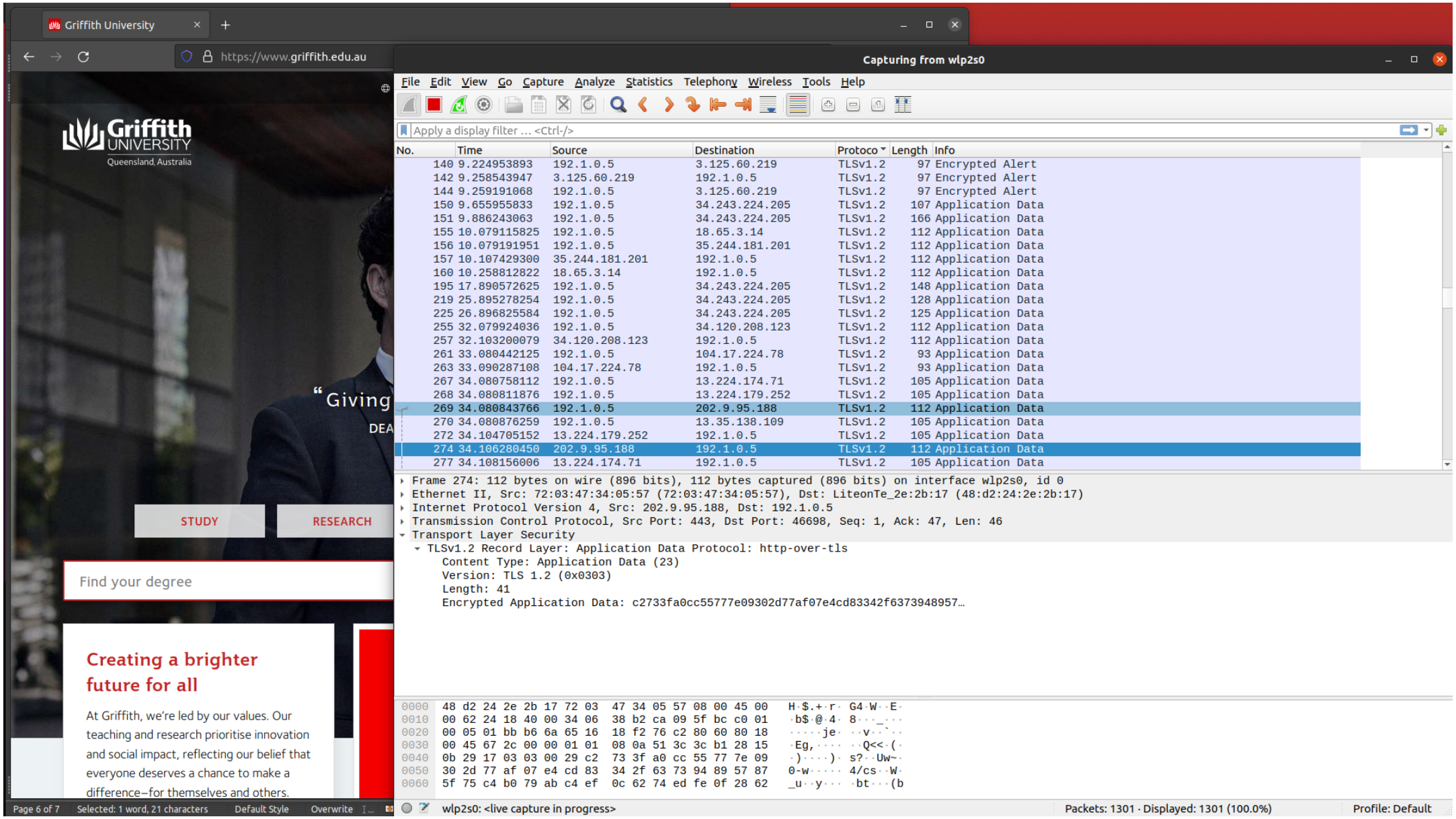
Q2: What is the TLS version used between your web browser and www.griffith.edu.au?

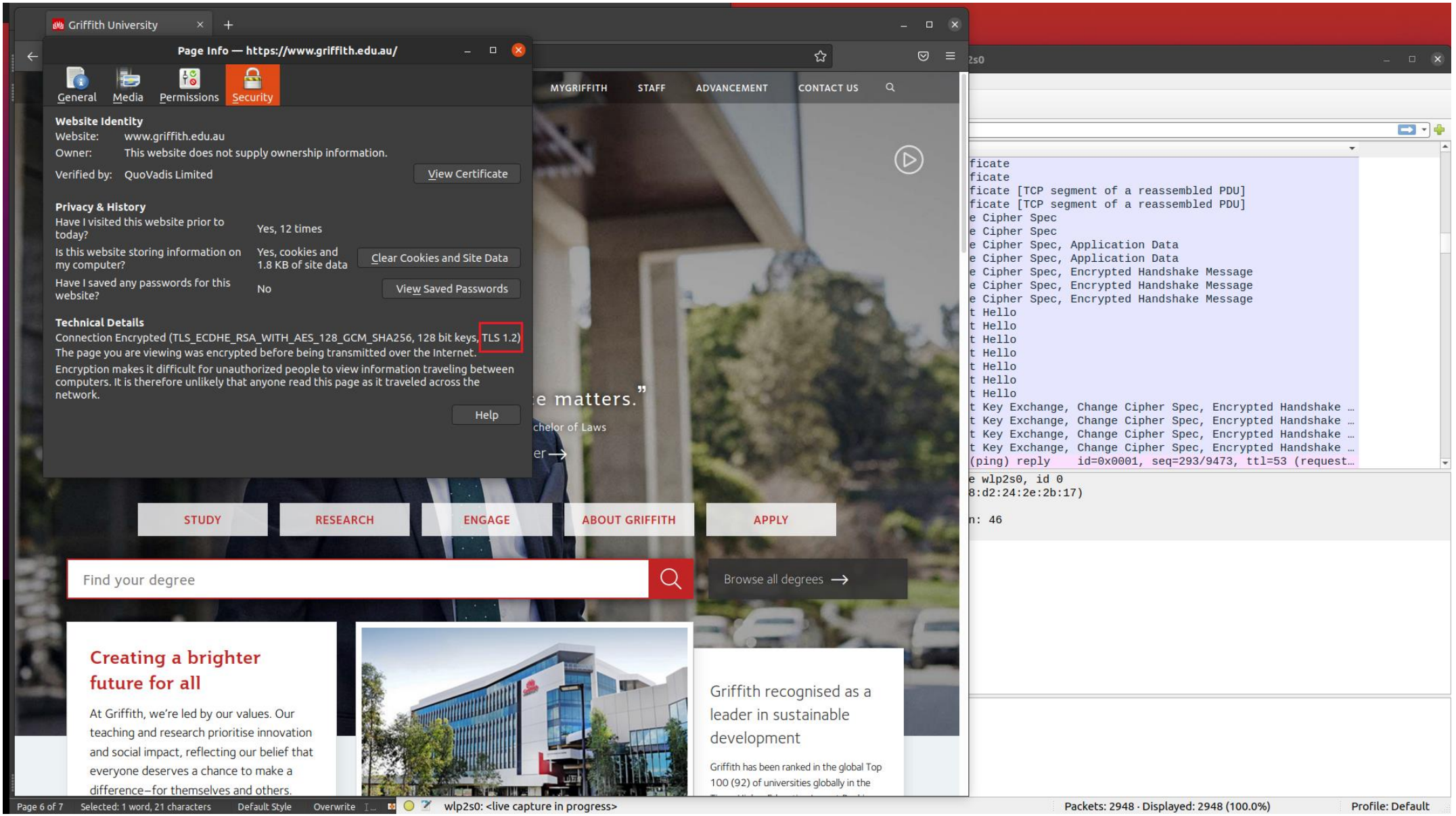
Answer:
TLSv1.2

My IP: 192.1.0.5


Settings
May 14 02:40
Settings
Wi-Fi
Connected
Wi-Fi
Network
Bluetooth
Background
Appearance
Notifications
Search
Applications
Privacy
Online Accounts
Sharing
Sound
Power
Screen Display
Mouse & Touchpad
Cancel
greengate
Apply
Details
Identity
IPv4
IPv6
Security
Signal Strength Good
Link speed 72 Mb/s (2.4 GHz)
Security WPA, WPA2
IPv4 Address 192.1.0.5
IPv6 Address fe80::8fb5:d1af:9d6d:b98e
Hardware Address 48:D2:24:2E:2B:17
Supported Frequencies 2.4 GHz
Default Route 192.1.0.254
DNS 192.1.0.254
Connect automatically
Make available to other users
Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.
Forget Connection

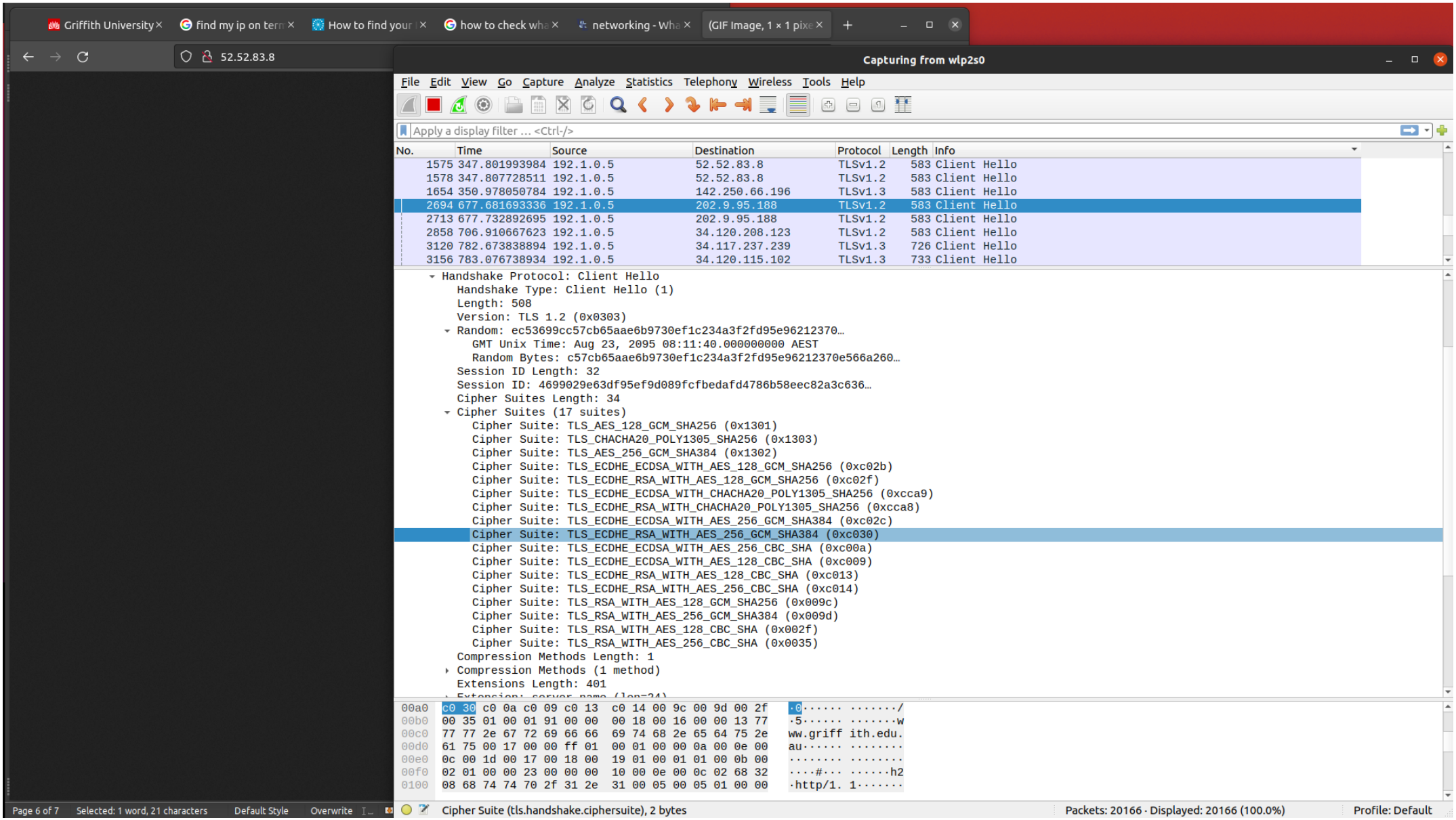

Griffith University
https://www.griffith.edu.au
Griffith UNIVERSITY
Queensland, Australia
“Giving
DEA
STUDY
RESEARCH
Find your degree
Creating a brighter future for all
At Griffith, we’re led by our values. Our teaching and research prioritise innovation and social impact, reflecting our belief that everyone deserves a chance to make a difference–for themselves and others.
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protoco Length Info
261 33.080442125 192.1.0.5 104.17.224.78 TLSv1.2 93 Application Data
263 33.090287108 104.17.224.78 192.1.0.5 TLSv1.2 93 Application Data
267 34.080758112 192.1.0.5 13.224.174.71 TLSv1.2 105 Application Data
268 34.080811876 192.1.0.5 13.224.179.252 TLSv1.2 105 Application Data
269 34.080843766 192.1.0.5 202.9.95.188 TLSv1.2 112 Application Data
270 34.080876259 192.1.0.5 13.35.138.109 TLSv1.2 105 Application Data
272 34.104705152 13.224.179.252 192.1.0.5 TLSv1.2 105 Application Data
274 34.106280450 202.9.95.188 192.1.0.5 TLSv1.2 112 Application Data
277 34.108156006 13.224.174.71 192.1.0.5 TLSv1.2 105 Application Data
280 34.109659887 13.35.138.109 192.1.0.5 TLSv1.2 105 Application Data
284 34.900737829 192.1.0.5 34.243.224.205 TLSv1.2 142 Application Data
287 35.081553253 192.1.0.5 35.186.226.184 TLSv1.2 105 Application Data
288 35.081772512 192.1.0.5 115.178.9.19 TLSv1.2 105 Application Data
290 35.105124809 35.186.226.184 192.1.0.5 TLSv1.2 105 Application Data
291 35.111142686 115.178.9.19 192.1.0.5 TLSv1.2 105 Application Data
295 35.902538315 192.1.0.5 34.243.224.205 TLSv1.2 157 Application Data
298 36.082056084 192.1.0.5 13.224.174.124 TLSv1.2 105 Application Data
299 36.082126229 192.1.0.5 13.107.21.200 TLSv1.2 100 Application Data
300 36.082164622 192.1.0.5 13.224.174.100 TLSv1.2 105 Application Data
301 36.082190956 192.1.0.5 13.35.138.111 TLSv1.2 105 Application Data
302 36.082274546 192.1.0.5 13.107.42.14 TLSv1.2 100 Application Data
305 36.107794345 13.107.21.200 192.1.0.5 TLSv1.2 100 Application Data
307 36.107839471 13.224.174.124 192.1.0.5 TLSv1.2 105 Application Data
Frame 269: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface wlp2s0, id 0
Ethernet II, Src: LiteonTe_2e:2b:17 (48:d2:24:2e:2b:17), Dst: 72:03:47:34:05:57 (72:03:47:34:05:57)
Internet Protocol Version 4, Src: 192.1.0.5, Dst: 202.9.95.188
Transmission Control Protocol, Src Port: 46698, Dst Port: 443, Seq: 1, Ack: 1, Len: 46
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 41
Encrypted Application Data: 0000000000000045b0716c6468d5258e907d6a9c45a1f139…
0000 72 03 47 34 05 57 48 d2 24 2e 2b 17 08 00 45 00
0010 00 62 2f ec 40 00 40 06 20 de c0 01 00 05 ca 09
0020 5f bc b6 6a 01 bb 76 c2 80 32 65 16 18 f2 80 18
0030 19 30 8b 8e 00 00 01 01 08 0a 28 15 0b 29 51 3b
0040 56 eb 17 03 03 00 29 00 00 00 00 00 00 00 45 b0
0050 71 6c 64 68 d5 25 8e 90 7d 6a 9c 45 a1 f1 39 39
0060 dc 1d c5 b8 a5 22 f2 e5 8e 9f 6a b5 5d c7 97 5f
wlp2s0: <live capture in progress>
Packets: 1195 · Displayed: 1195 (100.0%)
Profile: Default

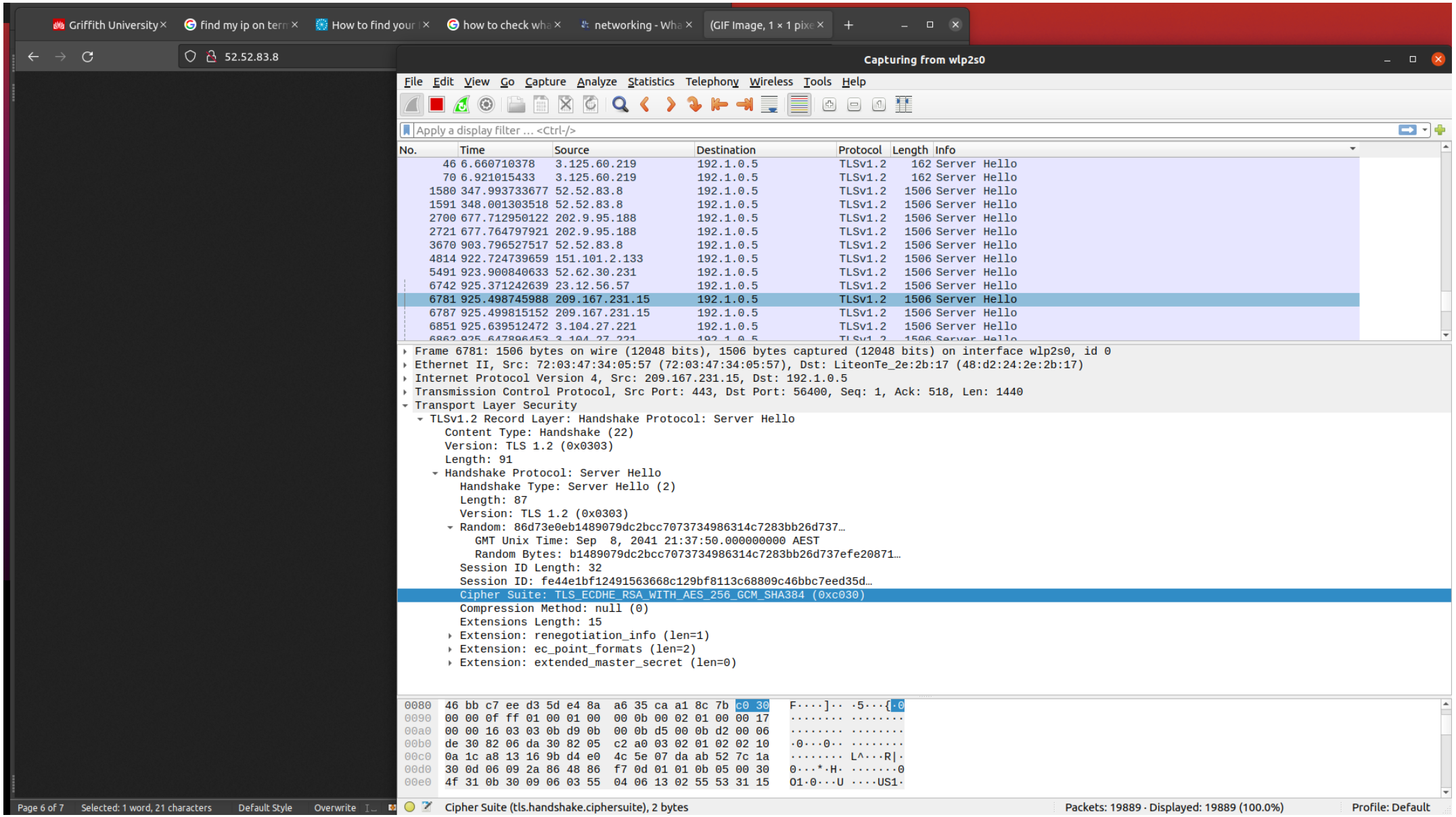

Griffith University
https://www.griffith.edu.au
Griffith UNIVERSITY
Queensland, Australia
"Giving
DEA
STUDY
RESEARCH
Find your degree
Creating a brighter future for all
At Griffith, we're led by our values. Our teaching and research prioritise innovation and social impact, reflecting our belief that everyone deserves a chance to make a difference–for themselves and others.
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protoco Length Info
140 9.224953893 192.1.0.5 3.125.60.219 TLSv1.2 97 Encrypted Alert
142 9.258543947 3.125.60.219 192.1.0.5 TLSv1.2 97 Encrypted Alert
144 9.259191068 192.1.0.5 3.125.60.219 TLSv1.2 97 Encrypted Alert
150 9.655955833 192.1.0.5 34.243.224.205 TLSv1.2 107 Application Data
151 9.886243063 192.1.0.5 34.243.224.205 TLSv1.2 166 Application Data
155 10.079115825 192.1.0.5 18.65.3.14 TLSv1.2 112 Application Data
156 10.079191951 192.1.0.5 35.244.181.201 TLSv1.2 112 Application Data
157 10.107429300 35.244.181.201 192.1.0.5 TLSv1.2 112 Application Data
160 10.258812822 18.65.3.14 192.1.0.5 TLSv1.2 112 Application Data
195 17.890572625 192.1.0.5 34.243.224.205 TLSv1.2 148 Application Data
219 25.895278254 192.1.0.5 34.243.224.205 TLSv1.2 128 Application Data
225 26.896825584 192.1.0.5 34.243.224.205 TLSv1.2 125 Application Data
255 32.079924036 192.1.0.5 34.120.208.123 TLSv1.2 112 Application Data
257 32.103200079 34.120.208.123 192.1.0.5 TLSv1.2 112 Application Data
261 33.080442125 192.1.0.5 104.17.224.78 TLSv1.2 93 Application Data
263 33.090287108 104.17.224.78 192.1.0.5 TLSv1.2 93 Application Data
267 34.080758112 192.1.0.5 13.224.174.71 TLSv1.2 105 Application Data
268 34.080811876 192.1.0.5 13.224.179.252 TLSv1.2 105 Application Data
269 34.080843766 192.1.0.5 202.9.95.188 TLSv1.2 112 Application Data
270 34.080876259 192.1.0.5 13.35.138.109 TLSv1.2 105 Application Data
272 34.104705152 13.224.179.252 192.1.0.5 TLSv1.2 105 Application Data
274 34.106280450 202.9.95.188 192.1.0.5 TLSv1.2 112 Application Data
277 34.108156006 13.224.174.71 192.1.0.5 TLSv1.2 105 Application Data
Frame 274: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface wlp2s0, id 0
Ethernet II, Src: 72:03:47:34:05:57 (72:03:47:34:05:57), Dst: LiteonTe_2e:2b:17 (48:d2:24:2e:2b:17)
Internet Protocol Version 4, Src: 202.9.95.188, Dst: 192.1.0.5
Transmission Control Protocol, Src Port: 443, Dst Port: 46698, Seq: 1, Ack: 47, Len: 46
Transport Layer Security
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 41
Encrypted Application Data: c2733fa0cc55777e09302d77af07e4cd83342f6373948957…
0000 48 d2 24 2e 2b 17 72 03 47 34 05 57 08 00 45 00 H·$.+·r· G4·W··E·
0010 00 62 24 18 40 00 34 06 38 b2 ca 09 5f bc c0 01 ·b$·@·4· 8···_···
0020 00 05 01 bb b6 6a 65 16 18 f2 76 c2 80 60 80 18 ·····je· ··v··`··
0030 00 45 67 2c 00 00 01 01 08 0a 51 3c 3c b1 28 15 ·Eg,···· ··Q<<·(·
0040 0b 29 17 03 03 00 29 c2 73 3f a0 cc 55 77 7e 09 ·)····)· s?··Uw~·
0050 30 2d 77 af 07 e4 cd 83 34 2f 63 73 94 89 57 87 0-w····· 4/cs··W·
0060 5f 75 c4 b0 79 ab c4 ef 0c 62 74 ed fe 0f 28 62 _u··y··· ·bt···(b
wlp2s0: <live capture in progress>
Packets: 1301 · Displayed: 1301 (100.0%)
Profile: Default


Griffith University
Page Info — https://www.griffith.edu.au/
General
Media
Permissions
Security
Website Identity
Website: www.griffith.edu.au
Owner: This website does not supply ownership information.
Verified by: QuoVadis Limited
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 12 times
Is this website storing information on my computer? Yes, cookies and 1.8 KB of site data
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help
MYGRIFFITH
STAFF
ADVANCEMENT
CONTACT US
STUDY
RESEARCH
ENGAGE
ABOUT GRIFFITH
APPLY
Find your degree
Browse all degrees
Creating a brighter future for all
At Griffith, we're led by our values. Our teaching and research prioritise innovation and social impact, reflecting our belief that everyone deserves a chance to make a difference–for themselves and others.
Griffith recognised as a leader in sustainable development
Griffith has been ranked in the global Top 100 (92) of universities globally in the
ficate
ficate
ficate [TCP segment of a reassembled PDU]
ficate [TCP segment of a reassembled PDU]
e Cipher Spec
e Cipher Spec
e Cipher Spec, Application Data
e Cipher Spec, Application Data
e Cipher Spec, Encrypted Handshake Message
e Cipher Spec, Encrypted Handshake Message
e Cipher Spec, Encrypted Handshake Message
t Hello
t Hello
t Hello
t Hello
t Hello
t Hello
t Hello
t Key Exchange, Change Cipher Spec, Encrypted Handshake …
t Key Exchange, Change Cipher Spec, Encrypted Handshake …
t Key Exchange, Change Cipher Spec, Encrypted Handshake …
t Key Exchange, Change Cipher Spec, Encrypted Handshake …
(ping) reply id=0x0001, seq=293/9473, ttl=53 (request…
e wlp2s0, id 0
8:d2:24:2e:2b:17)
n: 46
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite
wlp2s0: <live capture in progress>
Packets: 2948 · Displayed: 2948 (100.0%)
Profile: Default

Q3: What are the options of cipher suits your web browser picked? (Take a screenshot)

Answer:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

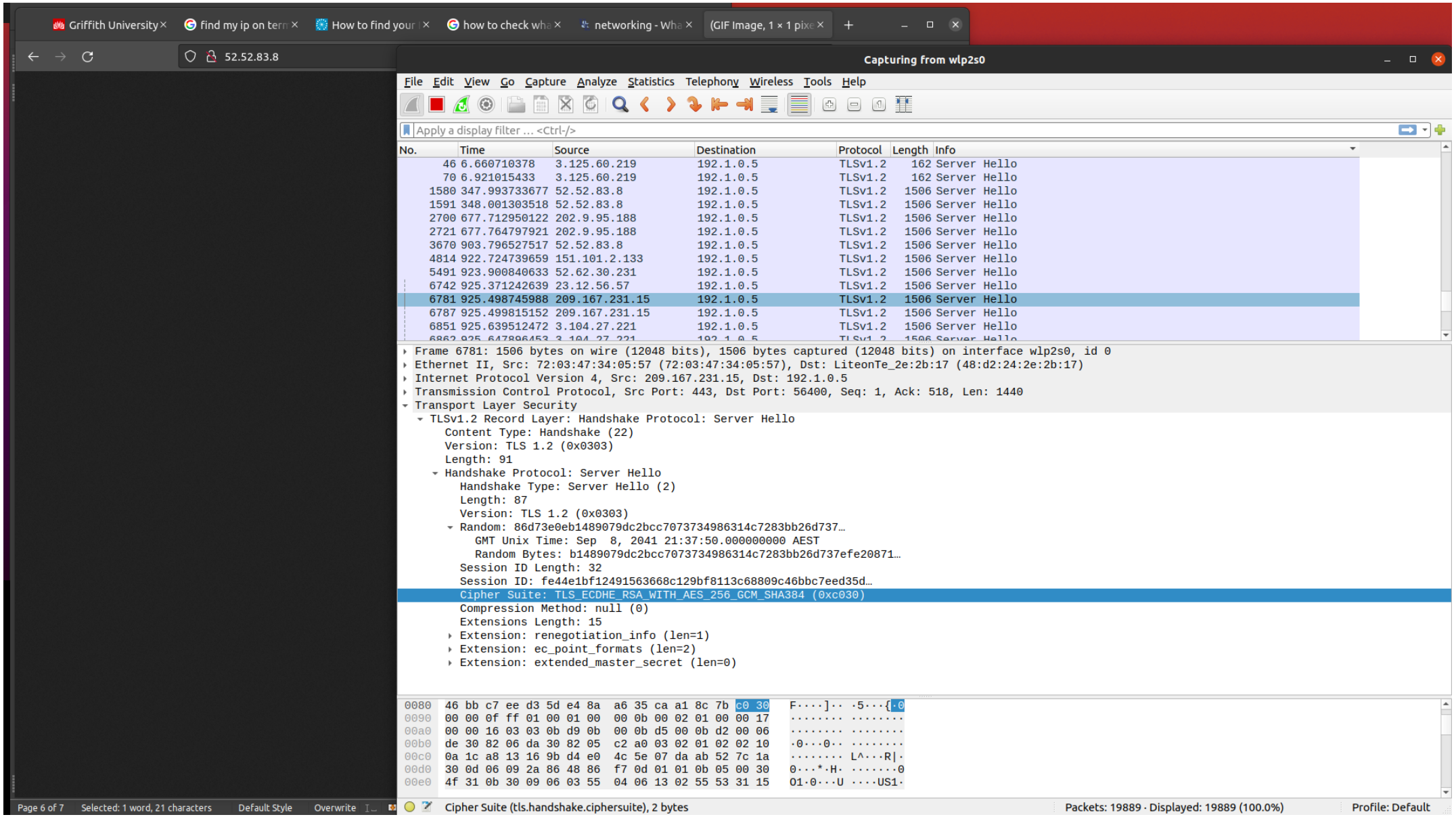

Griffith University
find my ip on tern
How to find your
how to check wha
networking - Wha
(GIF Image, 1 × 1 pixe
52.52.83.8
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1575 347.801993984 192.1.0.5 52.52.83.8 TLSv1.2 583 Client Hello
1578 347.807728511 192.1.0.5 52.52.83.8 TLSv1.2 583 Client Hello
1654 350.978050784 192.1.0.5 142.250.66.196 TLSv1.3 583 Client Hello
2694 677.681693336 192.1.0.5 202.9.95.188 TLSv1.2 583 Client Hello
2713 677.732892695 192.1.0.5 202.9.95.188 TLSv1.2 583 Client Hello
2858 706.910667623 192.1.0.5 34.120.208.123 TLSv1.2 583 Client Hello
3120 782.673838894 192.1.0.5 34.117.237.239 TLSv1.3 726 Client Hello
3156 783.076738934 192.1.0.5 34.120.115.102 TLSv1.3 733 Client Hello
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: ec53699cc57cb65aae6b9730ef1c234a3f2fd95e96212370…
GMT Unix Time: Aug 23, 2095 08:11:40.000000000 AEST
Random Bytes: c57cb65aae6b9730ef1c234a3f2fd95e96212370e566a260…
Session ID Length: 32
Session ID: 4699029e63df95ef9d089fcfbedafd4786b58eec82a3c636…
Cipher Suites Length: 34
Cipher Suites (17 suites)
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Compression Methods Length: 1
Compression Methods (1 method)
Extensions Length: 401
00a0 c0 30 c0 0a c0 09 c0 13 c0 14 00 9c 00 9d 00 2f
00b0 00 35 01 00 01 91 00 00 00 18 00 16 00 00 13 77
00c0 77 77 2e 67 72 69 66 66 69 74 68 2e 65 64 75 2e
00d0 61 75 00 17 00 00 ff 01 00 01 00 00 0a 00 0e 00
00e0 0c 00 1d 00 17 00 18 00 19 01 00 01 01 00 0b 00
00f0 02 01 00 00 23 00 00 00 10 00 0e 00 0c 02 68 32
0100 08 68 74 74 70 2f 31 2e 31 00 05 00 05 01 00 00
Cipher Suite (tls.handshake.ciphersuite), 2 bytes
Packets: 20166 · Displayed: 20166 (100.0%)
Profile: Default
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite


Griffith University
find my ip on tern
How to find your
how to check wha
networking - Wha
(GIF Image, 1 × 1 pixe
52.52.83.8
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
46 6.660710378 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
70 6.921015433 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
1580 347.993733677 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
1591 348.001303518 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
2700 677.712950122 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
2721 677.764797921 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
3670 903.796527517 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
4814 922.724739659 151.101.2.133 192.1.0.5 TLSv1.2 1506 Server Hello
5491 923.900840633 52.62.30.231 192.1.0.5 TLSv1.2 1506 Server Hello
6742 925.371242639 23.12.56.57 192.1.0.5 TLSv1.2 1506 Server Hello
6781 925.498745988 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6787 925.499815152 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6851 925.639512472 3.104.27.221 192.1.0.5 TLSv1.2 1506 Server Hello
Frame 6781: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface wlp2s0, id 0
Ethernet II, Src: 72:03:47:34:05:57 (72:03:47:34:05:57), Dst: LiteonTe_2e:2b:17 (48:d2:24:2e:2b:17)
Internet Protocol Version 4, Src: 209.167.231.15, Dst: 192.1.0.5
Transmission Control Protocol, Src Port: 443, Dst Port: 56400, Seq: 1, Ack: 518, Len: 1440
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 91
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 87
Version: TLS 1.2 (0x0303)
Random: 86d73e0eb1489079dc2bcc7073734986314c7283bb26d737…
GMT Unix Time: Sep 8, 2041 21:37:50.000000000 AEST
Random Bytes: b1489079dc2bcc7073734986314c7283bb26d737efe20871…
Session ID Length: 32
Session ID: fe44e1bf12491563668c129bf8113c68809c46bbc7eed35d…
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 15
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=2)
Extension: extended_master_secret (len=0)
0080 46 bb c7 ee d3 5d e4 8a a6 35 ca a1 8c 7b c0 30 F····]·· ·5···{·0
0090 00 00 0f ff 01 00 01 00 00 0b 00 02 01 00 00 17 ···· ····
00a0 00 00 16 03 03 0b d9 0b 00 0b d5 00 0b d2 00 06 ···· ····
00b0 de 30 82 06 da 30 82 05 c2 a0 03 02 01 02 02 10 ·0···0·· ····
00c0 0a 1c a8 13 16 9b d4 e0 4c 5e 07 da ab 52 7c 1a ···· L^···R|·
00d0 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 0···*·H· ····0
00e0 4f 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 O1·0···U ····US1·
Cipher Suite (tls.handshake.ciphersuite), 2 bytes
Packets: 19889 · Displayed: 19889 (100.0%)
Profile: Default
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite

Q4: What is the key exchange (delivery) method finally used, RSA encryption or Diffie-Hellman Key Exchange? (Take a screenshot to show this.)

Answer:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Elliptic Curve Diffie-Hellman, this protocol can have a smaller modulus than the classical Diffie-Hellman yet run faster and offer more security at the same time.

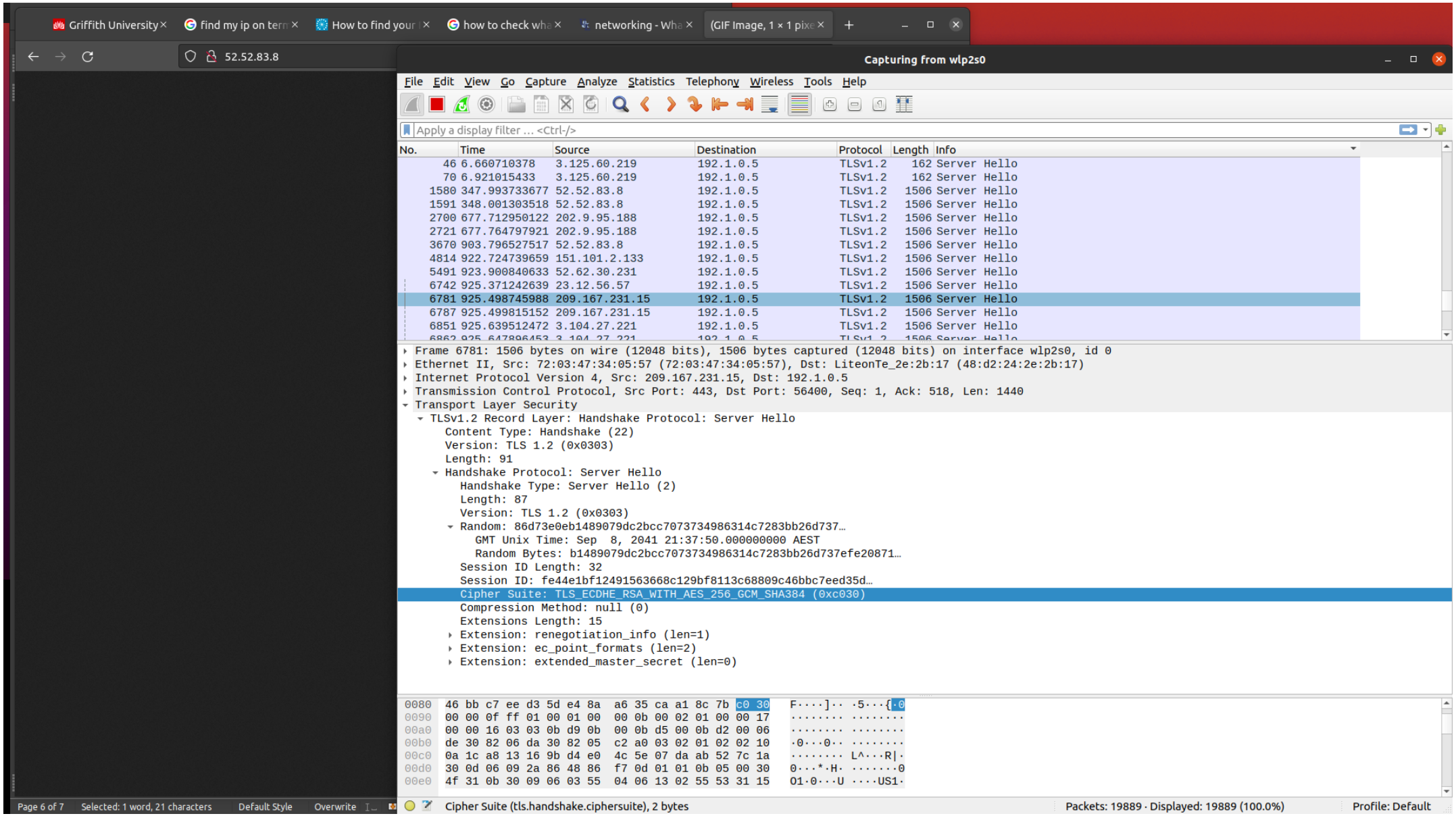

Griffith University
find my ip on tern
How to find your
how to check wha
networking - Wha
(GIF Image, 1 × 1 pixe
52.52.83.8
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
46 6.660710378 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
70 6.921015433 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
1580 347.993733677 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
1591 348.001303518 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
2700 677.712950122 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
2721 677.764797921 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
3670 903.796527517 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
4814 922.724739659 151.101.2.133 192.1.0.5 TLSv1.2 1506 Server Hello
5491 923.900840633 52.62.30.231 192.1.0.5 TLSv1.2 1506 Server Hello
6742 925.371242639 23.12.56.57 192.1.0.5 TLSv1.2 1506 Server Hello
6781 925.498745988 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6787 925.499815152 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6851 925.639512472 3.104.27.221 192.1.0.5 TLSv1.2 1506 Server Hello
Frame 6781: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface wlp2s0, id 0
Ethernet II, Src: 72:03:47:34:05:57 (72:03:47:34:05:57), Dst: LiteonTe_2e:2b:17 (48:d2:24:2e:2b:17)
Internet Protocol Version 4, Src: 209.167.231.15, Dst: 192.1.0.5
Transmission Control Protocol, Src Port: 443, Dst Port: 56400, Seq: 1, Ack: 518, Len: 1440
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 91
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 87
Version: TLS 1.2 (0x0303)
Random: 86d73e0eb1489079dc2bcc7073734986314c7283bb26d737…
GMT Unix Time: Sep 8, 2041 21:37:50.000000000 AEST
Random Bytes: b1489079dc2bcc7073734986314c7283bb26d737efe20871…
Session ID Length: 32
Session ID: fe44e1bf12491563668c129bf8113c68809c46bbc7eed35d…
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 15
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=2)
Extension: extended_master_secret (len=0)
0080 46 bb c7 ee d3 5d e4 8a a6 35 ca a1 8c 7b c0 30 F····]·· ·5···{·0
0090 00 00 0f ff 01 00 01 00 00 0b 00 02 01 00 00 17 ···· ····
00a0 00 00 16 03 03 0b d9 0b 00 0b d5 00 0b d2 00 06 ···· ····
00b0 de 30 82 06 da 30 82 05 c2 a0 03 02 01 02 02 10 ·0···0·· ····
00c0 0a 1c a8 13 16 9b d4 e0 4c 5e 07 da ab 52 7c 1a ···· L^···R|·
00d0 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 0···*·H· ····0
00e0 4f 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 O1·0···U ····US1·
Cipher Suite (tls.handshake.ciphersuite), 2 bytes
Packets: 19889 · Displayed: 19889 (100.0%)
Profile: Default
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite

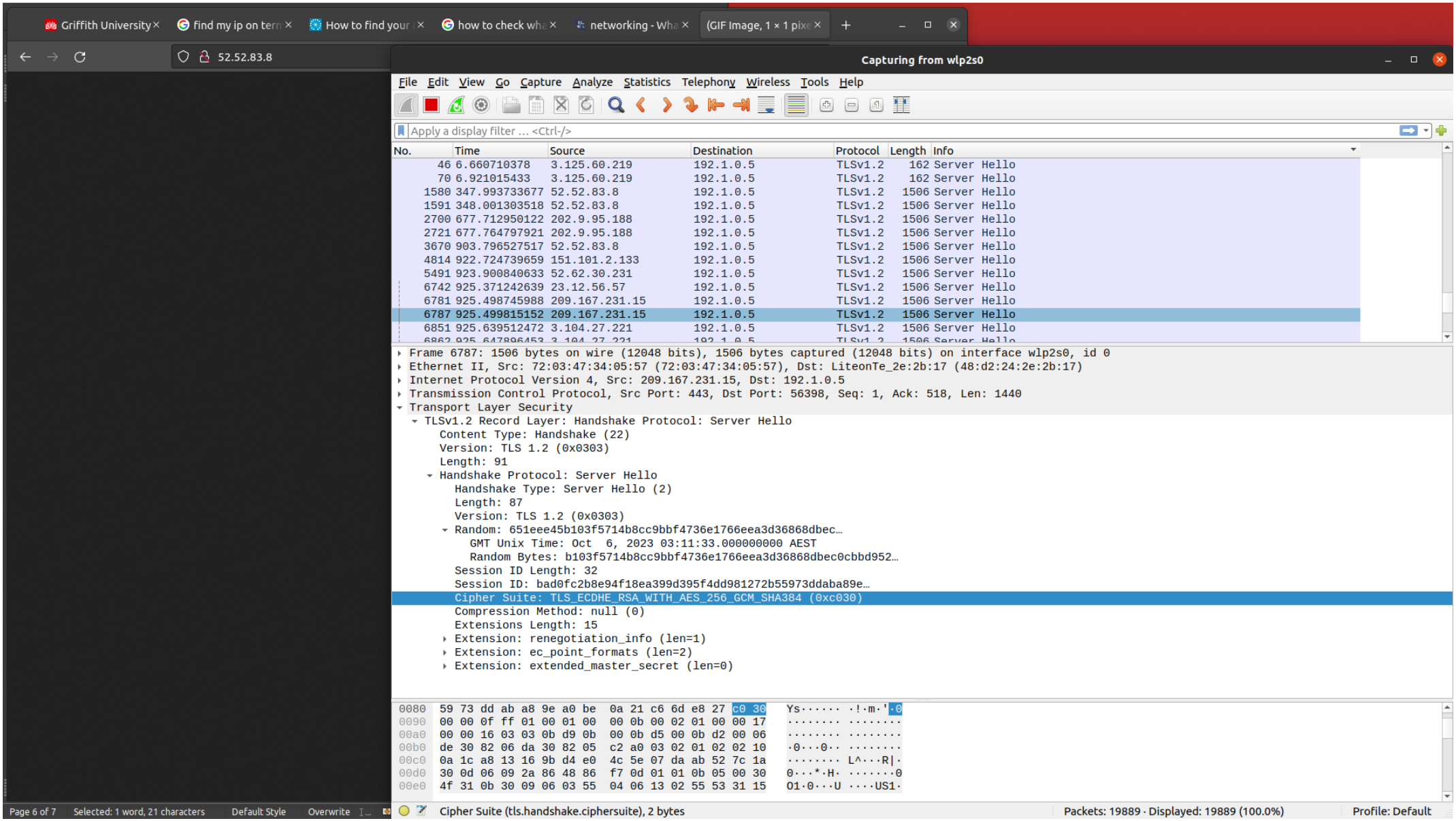
Q5: Does this TLS connection have forward secrecy? Why?

Answer:
Definitely because of the random numbers chosen with each session thanks to ECDHE

Server Hello
fe44e1bf12491563668c129bf8113c68809c46bbc7eed35de48aa635caa18c7b
bad0fc2b8e94f18ea399d395f4dd981272b55973ddaba89ea0be0a21c66de827

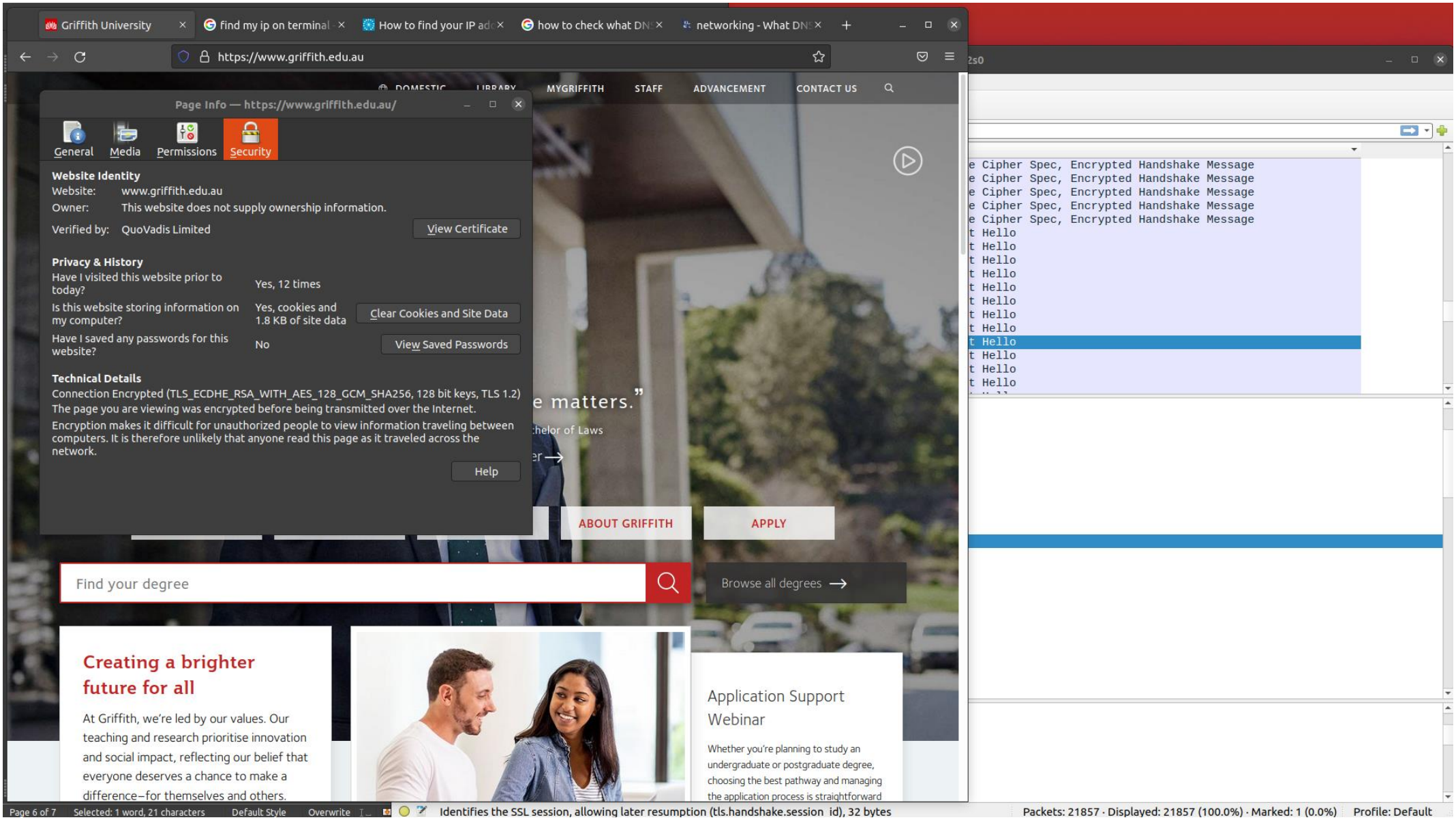
Client
4699029e63df95ef9d089fcfbedafd4786b58eec82a3c6361b81238362c1d534
5b3da3eaed147f45f250ef4a0e40a39647798e5c75e89a67705ee7ee7ce3821a

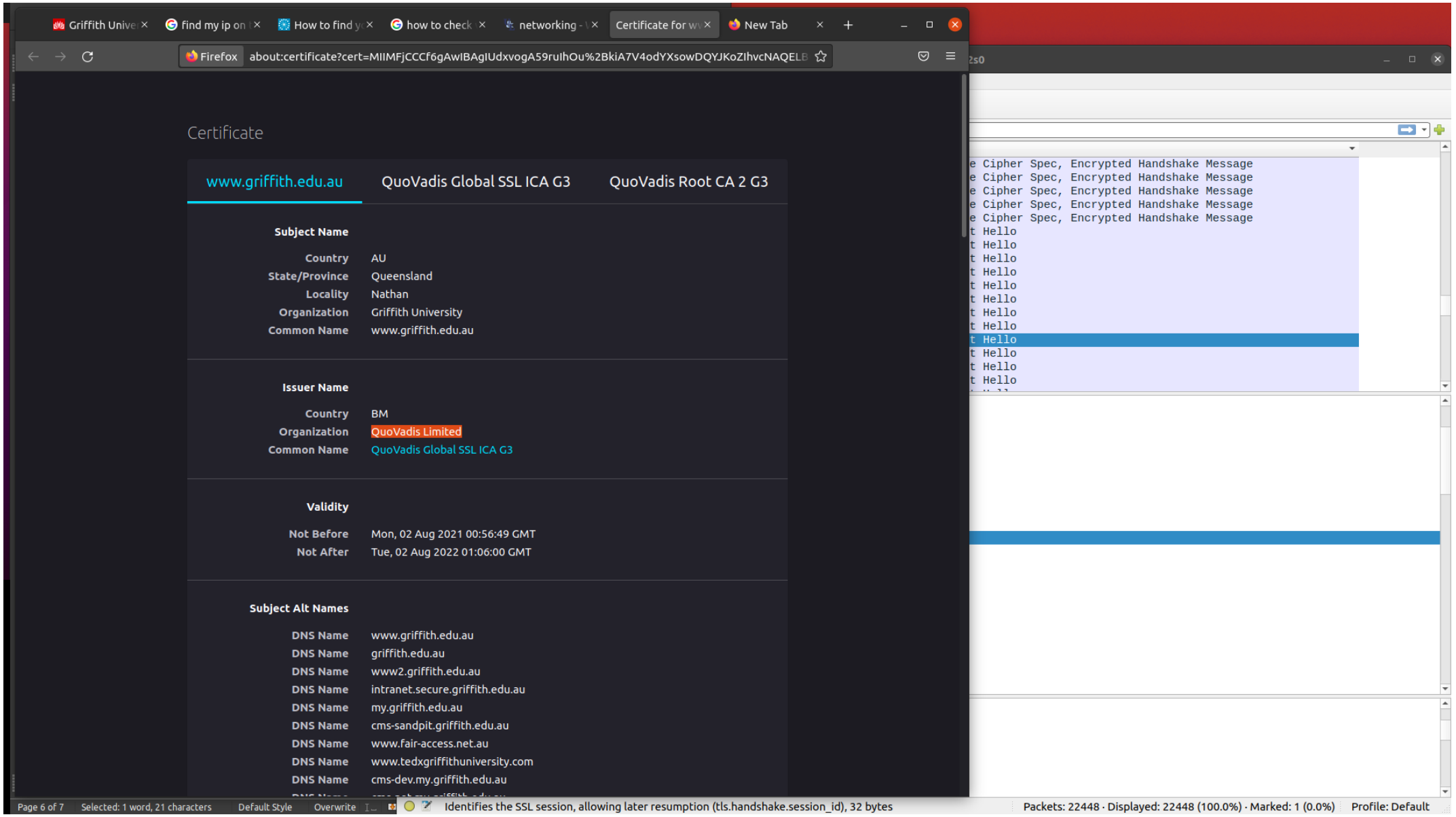

Griffith University
find my ip on tern
How to find your
how to check wha
networking - Wha
(GIF Image, 1 × 1 pixe
52.52.83.8
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
46 6.660710378 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
70 6.921015433 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
1580 347.993733677 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
1591 348.001303518 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
2700 677.712950122 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
2721 677.764797921 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
3670 903.796527517 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
4814 922.724739659 151.101.2.133 192.1.0.5 TLSv1.2 1506 Server Hello
5491 923.900840633 52.62.30.231 192.1.0.5 TLSv1.2 1506 Server Hello
6742 925.371242639 23.12.56.57 192.1.0.5 TLSv1.2 1506 Server Hello
6781 925.498745988 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6787 925.499815152 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6851 925.639512472 3.104.27.221 192.1.0.5 TLSv1.2 1506 Server Hello
Frame 6781: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface wlp2s0, id 0
Ethernet II, Src: 72:03:47:34:05:57 (72:03:47:34:05:57), Dst: LiteonTe_2e:2b:17 (48:d2:24:2e:2b:17)
Internet Protocol Version 4, Src: 209.167.231.15, Dst: 192.1.0.5
Transmission Control Protocol, Src Port: 443, Dst Port: 56400, Seq: 1, Ack: 518, Len: 1440
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 91
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 87
Version: TLS 1.2 (0x0303)
Random: 86d73e0eb1489079dc2bcc7073734986314c7283bb26d737…
GMT Unix Time: Sep 8, 2041 21:37:50.000000000 AEST
Random Bytes: b1489079dc2bcc7073734986314c7283bb26d737efe20871…
Session ID Length: 32
Session ID: fe44e1bf12491563668c129bf8113c68809c46bbc7eed35d…
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 15
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=2)
Extension: extended_master_secret (len=0)
0080 46 bb c7 ee d3 5d e4 8a a6 35 ca a1 8c 7b c0 30 F····]·· ·5···{·0
0090 00 00 0f ff 01 00 01 00 00 0b 00 02 01 00 00 17 ···· ····
00a0 00 00 16 03 03 0b d9 0b 00 0b d5 00 0b d2 00 06 ···· ····
00b0 de 30 82 06 da 30 82 05 c2 a0 03 02 01 02 02 10 ·0···0·· ····
00c0 0a 1c a8 13 16 9b d4 e0 4c 5e 07 da ab 52 7c 1a ···· L^···R|·
00d0 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 0···*·H· ····0
00e0 4f 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 O1·0···U ····US1·
Cipher Suite (tls.handshake.ciphersuite), 2 bytes
Packets: 19889 · Displayed: 19889 (100.0%)
Profile: Default
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite


Griffith University
find my ip on tern
How to find your
how to check wha
networking - Wha
(GIF Image, 1 × 1 pixe
52.52.83.8
Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
46 6.660710378 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
70 6.921015433 3.125.60.219 192.1.0.5 TLSv1.2 162 Server Hello
1580 347.993733677 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
1591 348.001303518 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
2700 677.712950122 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
2721 677.764797921 202.9.95.188 192.1.0.5 TLSv1.2 1506 Server Hello
3670 903.796527517 52.52.83.8 192.1.0.5 TLSv1.2 1506 Server Hello
4814 922.724739659 151.101.2.133 192.1.0.5 TLSv1.2 1506 Server Hello
5491 923.900840633 52.62.30.231 192.1.0.5 TLSv1.2 1506 Server Hello
6742 925.371242639 23.12.56.57 192.1.0.5 TLSv1.2 1506 Server Hello
6781 925.498745988 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6787 925.499815152 209.167.231.15 192.1.0.5 TLSv1.2 1506 Server Hello
6851 925.639512472 3.104.27.221 192.1.0.5 TLSv1.2 1506 Server Hello
Frame 6787: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface wlp2s0, id 0
Ethernet II, Src: 72:03:47:34:05:57 (72:03:47:34:05:57), Dst: LiteonTe_2e:2b:17 (48:d2:24:2e:2b:17)
Internet Protocol Version 4, Src: 209.167.231.15, Dst: 192.1.0.5
Transmission Control Protocol, Src Port: 443, Dst Port: 56398, Seq: 1, Ack: 518, Len: 1440
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 91
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 87
Version: TLS 1.2 (0x0303)
Random: 651eee45b103f5714b8cc9bbf4736e1766eea3d36868dbec…
GMT Unix Time: Oct 6, 2023 03:11:33.000000000 AEST
Random Bytes: b103f5714b8cc9bbf4736e1766eea3d36868dbec0cbbd952…
Session ID Length: 32
Session ID: bad0fc2b8e94f18ea399d395f4dd981272b55973ddaba89e…
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Compression Method: null (0)
Extensions Length: 15
Extension: renegotiation_info (len=1)
Extension: ec_point_formats (len=2)
Extension: extended_master_secret (len=0)
0080 59 73 dd ab a8 9e a0 be 0a 21 c6 6d e8 27 c0 30 Ys····· ·!·m·'·0
0090 00 00 0f ff 01 00 01 00 00 0b 00 02 01 00 00 17 ···· ····
00a0 00 00 16 03 03 0b d9 0b 00 0b d5 00 0b d2 00 06 ···· ····
00b0 de 30 82 06 da 30 82 05 c2 a0 03 02 01 02 02 10 ·0···0·· ····
00c0 0a 1c a8 13 16 9b d4 e0 4c 5e 07 da ab 52 7c 1a ···· L^···R|·
00d0 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 0···*·H· ····0
00e0 4f 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 15 O1·0···U ····US1·
Cipher Suite (tls.handshake.ciphersuite), 2 bytes
Packets: 19889 · Displayed: 19889 (100.0%)
Profile: Default
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite

Q6: What is the organisation name of the CA who issued certificate to www.griffith.edu.au?

Answer:
QuoVadis Limited

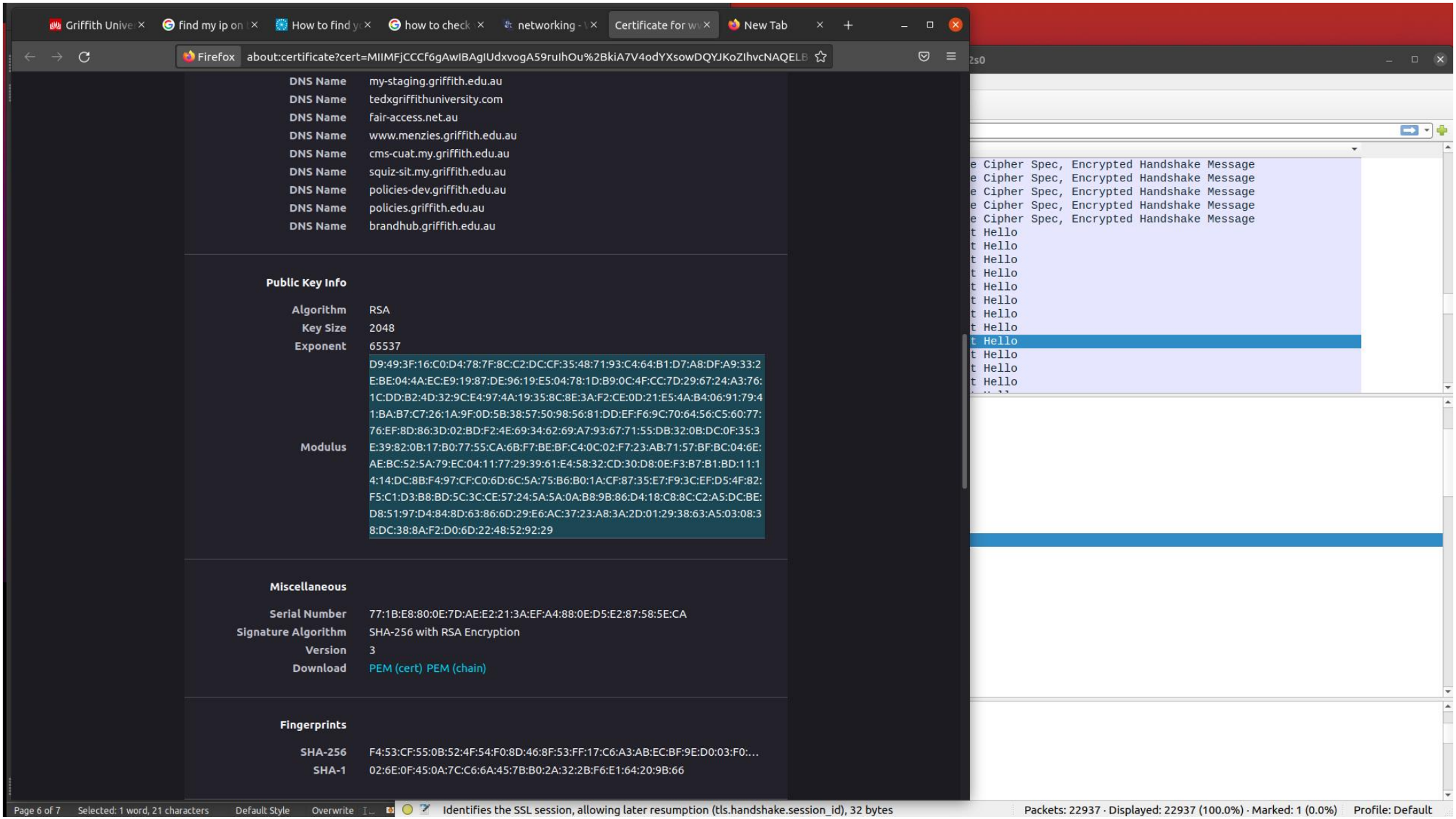

Griffith University
find my ip on terminal
How to find your IP ad
how to check what DN
networking - What DN
https://www.griffith.edu.au
DOMESTIC
LIBRARY
MYGRIFFITH
STAFF
ADVANCEMENT
CONTACT US
Page Info — https://www.griffith.edu.au/
General
Media
Permissions
Security
Website Identity
Website: www.griffith.edu.au
Owner: This website does not supply ownership information.
Verified by: QuoVadis Limited
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 12 times
Is this website storing information on my computer? Yes, cookies and 1.8 KB of site data
Clear Cookies and Site Data
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.
Help
e matters."
ABOUT GRIFFITH
APPLY
Find your degree
Browse all degrees
Creating a brighter future for all
At Griffith, we're led by our values. Our teaching and research prioritise innovation and social impact, reflecting our belief that everyone deserves a chance to make a difference–for themselves and others.
Application Support Webinar
Whether you're planning to study an undergraduate or postgraduate degree, choosing the best pathway and managing the application process is straightforward
e Cipher Spec, Encrypted Handshake Message
t Hello
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite
Identifies the SSL session, allowing later resumption (tls.handshake.session_id), 32 bytes
Packets: 21857 · Displayed: 21857 (100.0%) · Marked: 1 (0.0%)
Profile: Default


Griffith Unive
find my ip on
How to find y
how to check
networking -
Certificate for w
New Tab
Firefox
about:certificate?cert=MIIMFjCCCf6gAwIBAgIUdxvogA59ruIhOu%2BkiA7V4odYXsowDQYJKoZIhvcNAQELB
Certificate
www.griffith.edu.au
QuoVadis Global SSL ICA G3
QuoVadis Root CA 2 G3
Subject Name
Country AU
State/Province Queensland
Locality Nathan
Organization Griffith University
Common Name www.griffith.edu.au
Issuer Name
Country BM
Organization QuoVadis Limited
Common Name QuoVadis Global SSL ICA G3
Validity
Not Before Mon, 02 Aug 2021 00:56:49 GMT
Not After Tue, 02 Aug 2022 01:06:00 GMT
Subject Alt Names
DNS Name www.griffith.edu.au
DNS Name griffith.edu.au
DNS Name www2.griffith.edu.au
DNS Name intranet.secure.griffith.edu.au
DNS Name my.griffith.edu.au
DNS Name cms-sandpit.griffith.edu.au
DNS Name www.fair-access.net.au
DNS Name www.tedxgriffithuniversity.com
DNS Name cms-dev.my.griffith.edu.au
e Cipher Spec, Encrypted Handshake Message
t Hello
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite
Identifies the SSL session, allowing later resumption (tls.handshake.session_id), 32 bytes
Packets: 22448 · Displayed: 22448 (100.0%) · Marked: 1 (0.0%)
Profile: Default

Q7: What is the value of www.griffith.edu.au 's public key?

Answer:

D9:49:3F:16:C0:D4:78:7F:8C:C2:DC:CF:35:48:71:93:C4:64:B1:D7:A8:DF:A9:33:2
E:BE:04:4A:EC:E9:19:87:DE:96:19:E5:04:78:1D:B9:0C:4F:CC:7D:29:67:24:A3:76:
1C:DD:B2:4D:32:9C:E4:97:4A:19:35:8C:8E:3A:F2:CE:0D:21:E5:4A:B4:06:91:79:4
1:BA:B7:C7:26:1A:9F:0D:5B:38:57:50:98:56:81:DD:EF:F6:9C:70:64:56:C5:60:77:
76:EF:8D:86:3D:02:BD:F2:4E:69:34:62:69:A7:93:67:71:55:DB:32:0B:DC:0F:35:3
E:39:82:0B:17:B0:77:55:CA:6B:F7:BE:BF:C4:0C:02:F7:23:AB:71:57:BF:BC:04:6E:
AE:BC:52:5A:79:EC:04:11:77:29:39:61:E4:58:32:CD:30:D8:0E:F3:B7:B1:BD:11:1
4:14:DC:8B:F4:97:CF:C0:6D:6C:5A:75:B6:B0:1A:CF:87:35:E7:F9:3C:EF:D5:4F:82:
F5:C1:D3:B8:BD:5C:3C:CE:57:24:5A:5A:0A:B8:9B:86:D4:18:C8:8C:C2:A5:DC:BE:
D8:51:97:D4:84:8D:63:86:6D:29:E6:AC:37:23:A8:3A:2D:01:29:38:63:A5:03:08:3
8:DC:38:8A:F2:D0:6D:22:48:52:92:29


Griffith Unive
find my ip on
How to find y
how to check
networking - \
Certificate for w
New Tab
Firefox
about:certificate?cert=MIIMFjCCCf6gAwIBAgIUdxvogA59rulhOu%2BkiA7V4odYXsowDQYJKoZIhvcNAQELB
DNS Name my-staging.griffith.edu.au
DNS Name tedxgriffithuniversity.com
DNS Name fair-access.net.au
DNS Name www.menzies.griffith.edu.au
DNS Name cms-cuat.my.griffith.edu.au
DNS Name squiz-sit.my.griffith.edu.au
DNS Name policies-dev.griffith.edu.au
DNS Name policies.griffith.edu.au
DNS Name brandhub.griffith.edu.au
Public Key Info
Algorithm RSA
Key Size 2048
Exponent 65537
Modulus D9:49:3F:16:C0:D4:78:7F:8C:C2:DC:CF:35:48:71:93:C4:64:B1:D7:A8:DF:A9:33:2E:BE:04:4A:EC:E9:19:87:DE:96:19:E5:04:78:1D:B9:0C:4F:CC:7D:29:67:24:A3:76:1C:DD:B2:4D:32:9C:E4:97:4A:19:35:8C:8E:3A:F2:CE:0D:21:E5:4A:B4:06:91:79:41:BA:B7:C7:26:1A:9F:0D:5B:38:57:50:98:56:81:DD:EF:F6:9C:70:64:56:C5:60:77:76:EF:8D:86:3D:02:BD:F2:4E:69:34:62:69:A7:93:67:71:55:DB:32:0B:DC:0F:35:3E:39:82:0B:17:B0:77:55:CA:6B:F7:BE:BF:C4:0C:02:F7:23:AB:71:57:BF:BC:04:6E:AE:BC:52:5A:79:EC:04:11:77:29:39:61:E4:58:32:CD:30:D8:0E:F3:B7:B1:BD:11:14:14:DC:8B:F4:97:CF:C0:6D:6C:5A:75:B6:B0:1A:CF:87:35:E7:F9:3C:EF:D5:4F:82:F5:C1:D3:B8:BD:5C:3C:CE:57:24:5A:5A:0A:B8:9B:86:D4:18:C8:8C:C2:A5:DC:BE:D8:51:97:D4:84:8D:63:86:6D:29:E6:AC:37:23:A8:3A:2D:01:29:38:63:A5:03:08:38:DC:38:8A:F2:D0:6D:22:48:52:92:29
Miscellaneous
Serial Number 77:1B:E8:80:0E:7D:AE:E2:21:3A:EF:A4:88:0E:D5:E2:87:58:5E:CA
Signature Algorithm SHA-256 with RSA Encryption
Version 3
Download PEM (cert) PEM (chain)
Fingerprints
SHA-256 F4:53:CF:55:0B:52:4F:54:F0:8D:46:8F:53:FF:17:C6:A3:AB:EC:BF:9E:D0:03:F0:...
SHA-1 02:6E:0F:45:0A:7C:C6:6A:45:7B:B0:2A:32:2B:F6:E1:64:20:9B:66
e Cipher Spec, Encrypted Handshake Message
t Hello
Page 6 of 7
Selected: 1 word, 21 characters
Default Style
Overwrite
Identifies the SSL session, allowing later resumption (tls.handshake.session_id), 32 bytes
Packets: 22937 · Displayed: 22937 (100.0%) · Marked: 1 (0.0%)
Profile: Default

Q8: What are the symmetric-key cipher algorithm and operation mode used to encrypt the application data?

Answer:
AES_256_GCM

Using a 256 bit key, much more secure than what was used in previous laboratories

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Q9: Did the TLS handshake use mutual authentication? Does www.griffith.edu.au know it is you (as a university student with your student number) are connecting to it? How does the university server get to know who you are when you login and start accessing the course web sites?

Answer:
This connection was not based on mutual authentication as the university server did not request the PC used in this lab for a corticate.

However, if the utilization of the server's services are requested then the server will ask for user credentials on the application layer. User credentials will be sent encrypted in a so-called TLS session tunnel securely, in the record later with respect to the TLS session.

The transmitted user credentials will have the password hashed and compared to the stored hash values associated with the user. This happens in the Application layer of the OSI model.

This is the end of the workshop

Acknowledgement: This lab instruction is partially based on the SEED labs from the SEED project led by Professor Wenliang Du, Syracuse University.