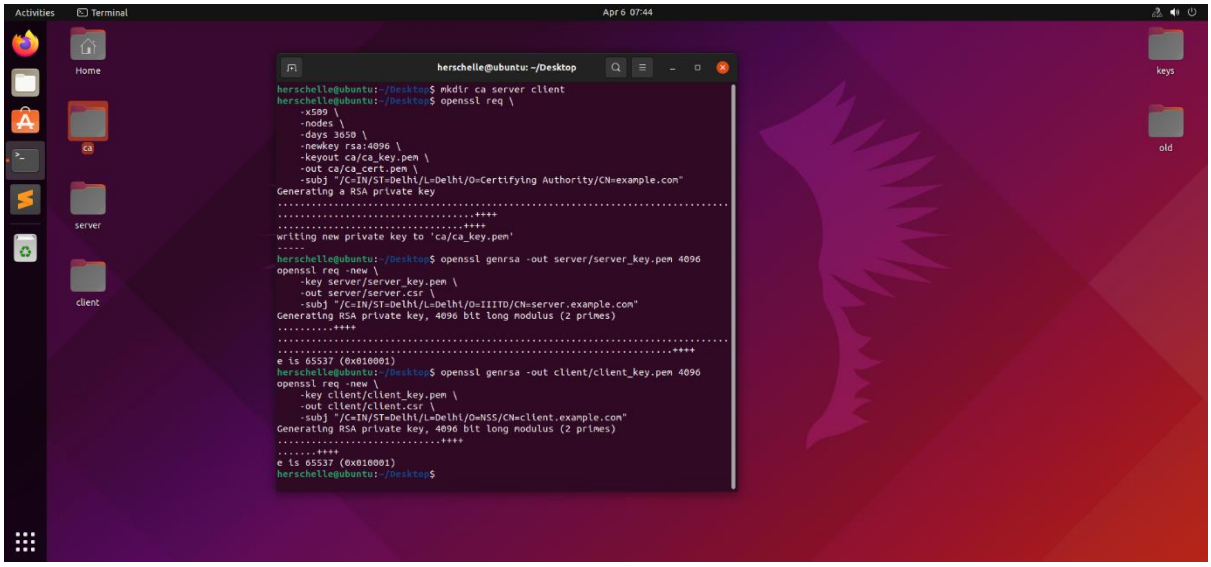
Task 1:

```
openssl req \
   -x509 \                          #X.509 Standard
   -nodes \                         #No password protection
   -days 3650 \                     #Valid for 10yrs
   -newkey rsa:4096 \               #For creating new key
   -keyout ca/ca_key.pem \          #Key file of ca
   -out ca/ca_cert.pem \            #Certificate file of ca
   -subj "/C=IN/ST=Delhi/L=Delhi/O=Certifying Authority/CN=example.com"        #Other info

openssl genrsa -out server/server_key.pem 4096
openssl req -new \
   -key server/server_key.pem \
   -out server/server.csr \
   -subj "/C=IN/ST=Delhi/L=Delhi/O=IIITD/CN=server.example.com"


openssl genrsa -out client/client_key.pem 4096
openssl req -new \
   -key client/client_key.pem \
   -out client/client.csr \
   -subj "/C=IN/ST=Delhi/L=Delhi/O=NSS/CN=client.example.com"
```



openssl x509 -req -days 1460 -in server/server.csr \

-CA ca/ca_cert.pem -CAkey ca/ca_key.pem \

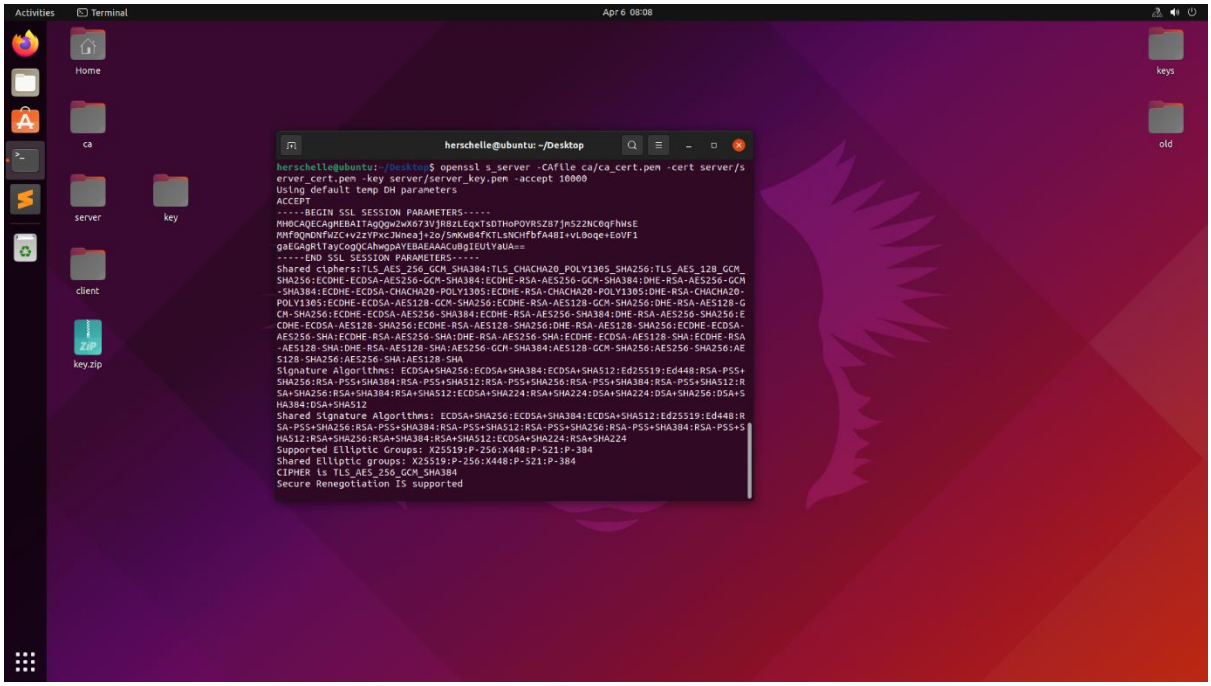
-CAcreateserial -out server/server_cert.pem

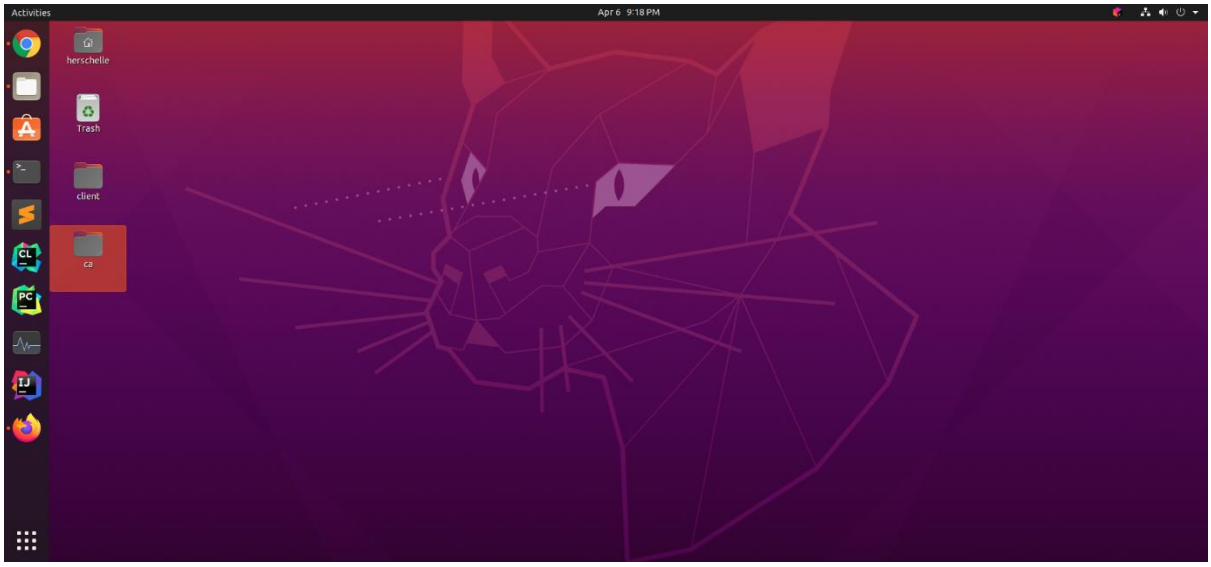
openssl x509 -req -days 1460 -in client/client.csr \

-CA ca/ca_cert.pem -CAkey ca/ca_key.pem \

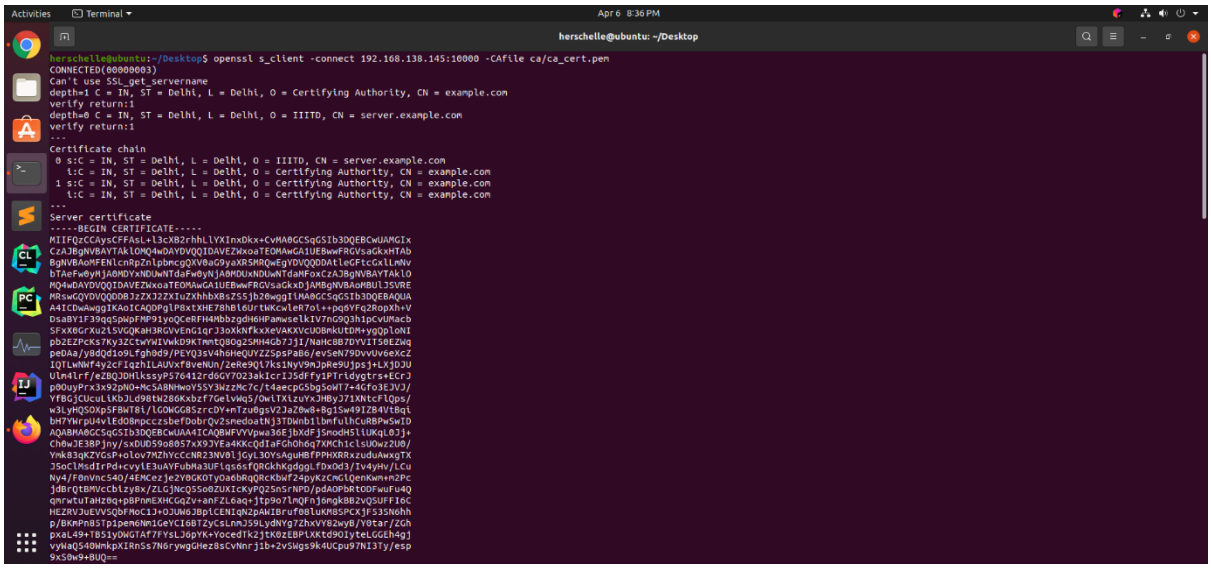
-CAcreateserial -out client/client_cert.pem

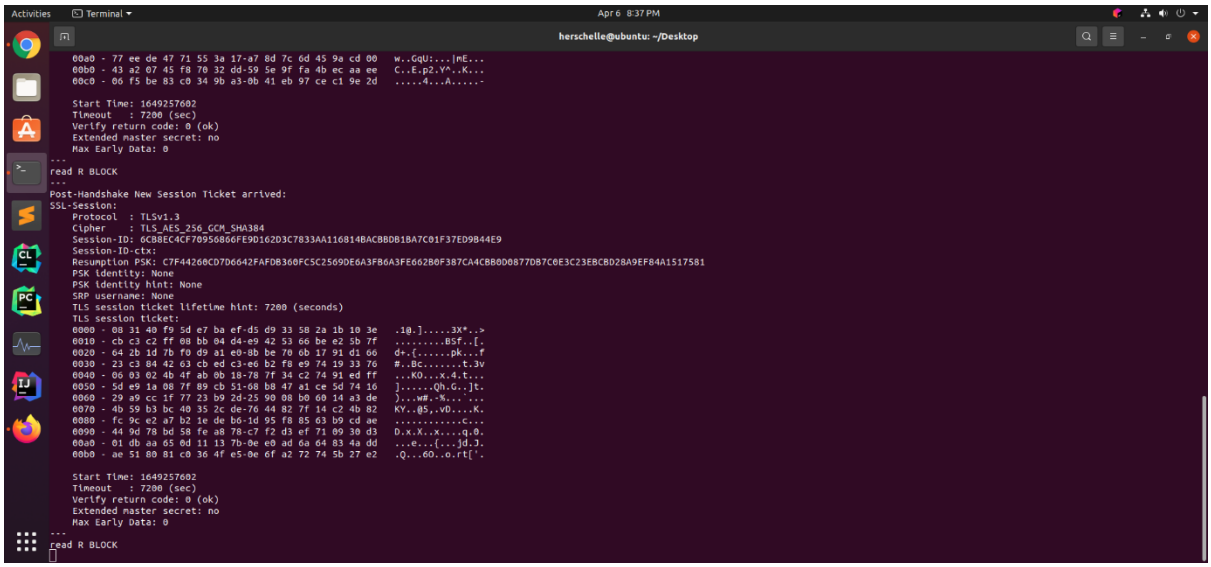
First we run without -Verify option. Copy the ca and client directory to second vm.

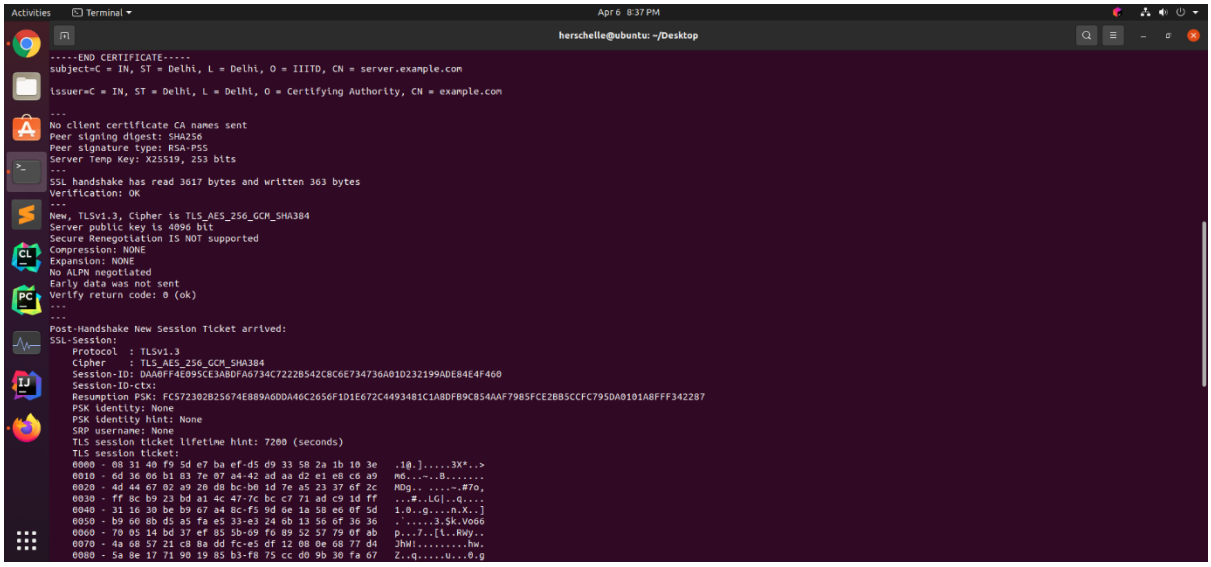




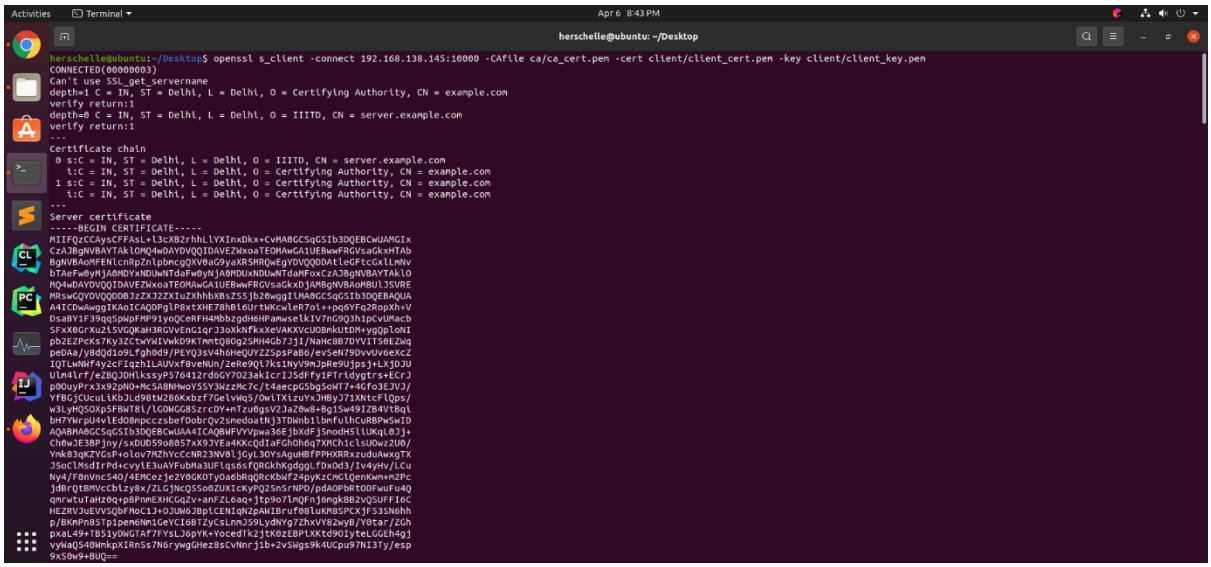
In this case we only enter the ca certificate and see the verify return code is 0



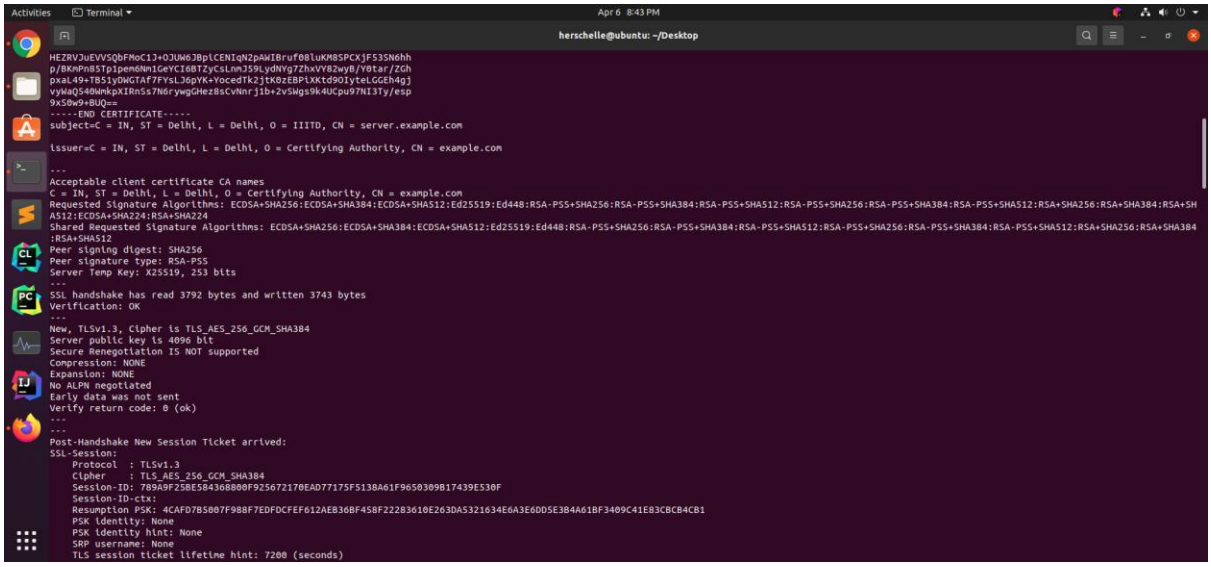


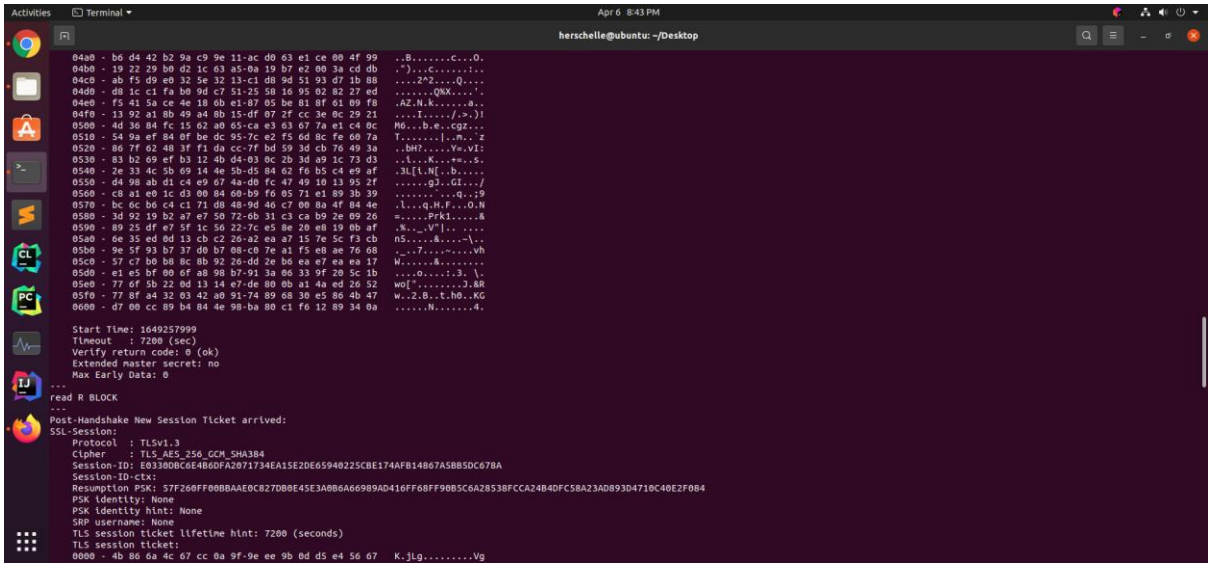


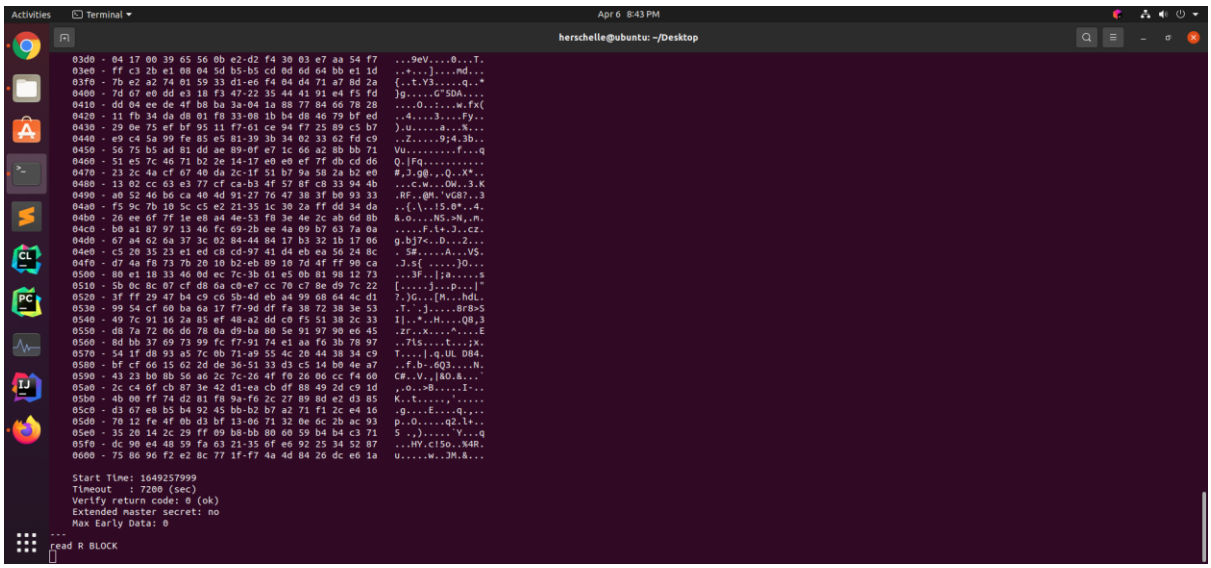
Now we put -Verify 1 option in the s_server and now in s_client we need to send client certificates as well, shown below



MIIFQzCCAysCFFAsL+ł3cXB2rhhLlYXInxDkx+CvMA0GCSqGSIb3DQEBCwUAMGIx
CzAJBgNVBAYTAklOMQ4wDAYDVQQIDAVEZWxoaTEOMAwGA1UEBwwFRGVsaGkxHTAb
BgNVBAoMFENlcnRpZmlzbmcgQXV0aG9yaXR5MRQwEgYDVQQDDAtleGFtcGxlLmNv
bTAeFw0yMjA0NDYxNDUwNTdaFw0yNjA0MDUxNDUwNTdaMFoxCzAJBgNVBAYTAklO
MQ4wDAYDVQQIDAVEZWxoaTEOMAwGA1UEBwwFRGVsaGkxDjAMBgNVBAoMBUl3SVRE
MRswGQYDVQQDDBJzZXJ2ZXIuZXhhbXBsZS5jb20wggIiMA0GCSqGSIb3DQEBAQUA
A4ICDwAwggIKAoICAQDRglP8xtXHE78hBi6UrtWKcwleR7oi++pq6YFq2RopXh+V
DsaBY1F39qqSpWpFfNP91yoQCeRFH4HbbzgdH6HPamwselkIV7nG9Q3h1pCvUMacb
SFxX6GrXu2lSVGQkaH3RGVvEnGiqrJ3oXkNfkxXeVAKXVcUOBmkUtDM+yqQploNI
pb2EZPcKs7Ky3ZCtwYWIVwkD9KTmmtQ8Og2SMH4Gb7J1I/NaHc8B7DYVIT50EZWq
peDAa/y8dQd1o9LfghOd9/PEYQ3sV4hOHeQUYZZSpsPaB6/evSeN79DvvUv6eXcZ
IQTLwNNf4y2cFIqzhILAUVxf8veNUn/2eRe9Qi7ks1NyV9mJpRe9Ujpsj+LXjDJU
Ul4lrf/eZBQJDHlkssyP57641Zr6GY7O23akIcrlJ5dffy1PTrldygtrs+ECrJ
p0OuyPrx3x9ZpNO+McS4BNHwoY55Y3WzzMc7c/t4eecpG5bgSoWT7+4Cfo3ILVJ/
YfBGjCUcuLiKbJLd98tW286KxbzF7GelvWq5/OwiTXizuYxJHByJ71XNtcFlQps/
w3LyHQSOXp5FBWT8l/lGOWGG8SzrcDY+mTzu0gsV2JaZ0w8+Bg1Sw49IZ84VtBqi
bH7YWrpU4vlEdO8npcczsbefDobrQv2smedoatNj3TDWnb1lbmfulhCuRBPwSwID
AQABMA0GCSqGSIb3DQEBCwUAA4ICAQBWFVVpwa36EjbXdFj5modH5liUKqL0Jj+
Ch0wJE3BPjny/sxDUD59o8057xX9JYE4HKcQdIaFGhOh6q7XMCh1c1sUOw22U0/
Ymk83qKZYGsP+olov7MZhYcCcNR23NV0ljGyL3OYsAguHBfPPHXRRxzuduAwxqTX
JSoClMsdIrPd+cvylE3uAYFubMa3UFlqs6sfQRGkhKgdggLfDxOd3/Iv4yHv/LCu
Ny4/F0nVnc54O/4EMCezje2Y0GKOTyOa6bRqQRcKbWf24pyKzCmGlQenKwn+m2Pc
jdBrQtBMVcCbizyBx/ZLGjNcQSSo0ZUXIcKyPQ2SnSrNPD/pdAOPbRtODFwuFu4Q
qnrwTuTaH2RQ+pBFnMEXHCGqZv+anFZL6aq+jtp9o7lnQFnjmgkBBIvQSUFI6CH
HEZRVJuEVVSQbFHoCiJ+OJUN6JBpiCENIqN2pAWIBrufB8lUKM8SPCXjF53SN6hh
p/BKmPn8STp1pem6Nm1GeYCIGBTZyCsLnmJS9LydNYg7ZhxVY82wyB/Y0tar/ZGh
pxaL49+TB51yDWGTAf7FYsLJ0pYK+YocedTk2jtK0zEBPlXKtd9OiyteLGGEh4gj
vyWaQS40WmkpXIRnSs7N6rywgGHez8sCvNnrj1b+2vSWgs9k4UCpu97NI3Ty/esp
9x50w9+BUQ==



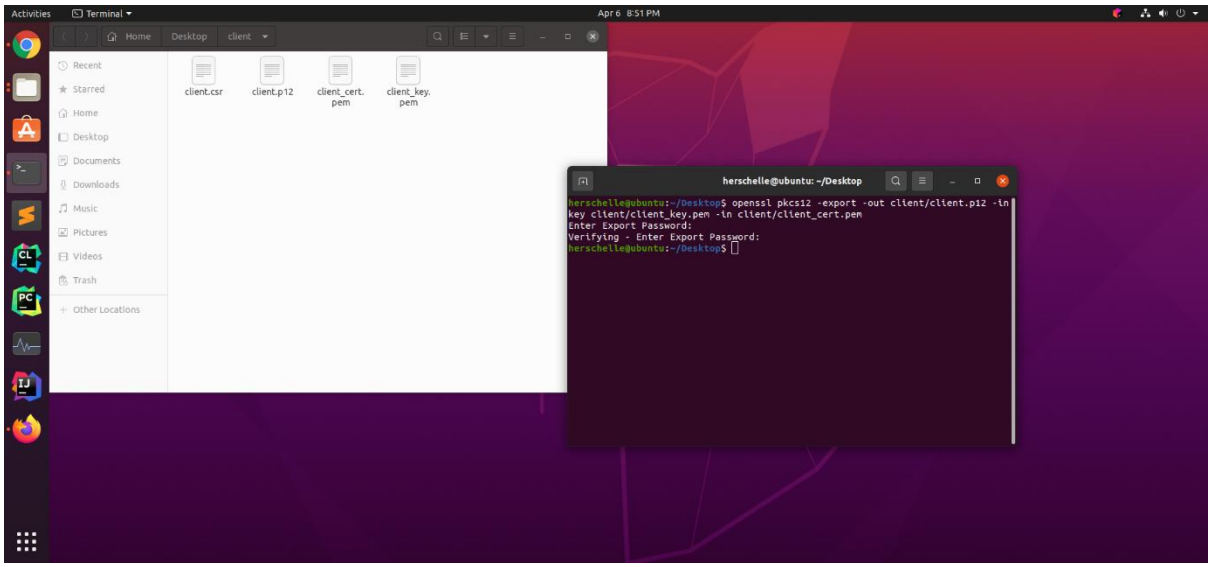




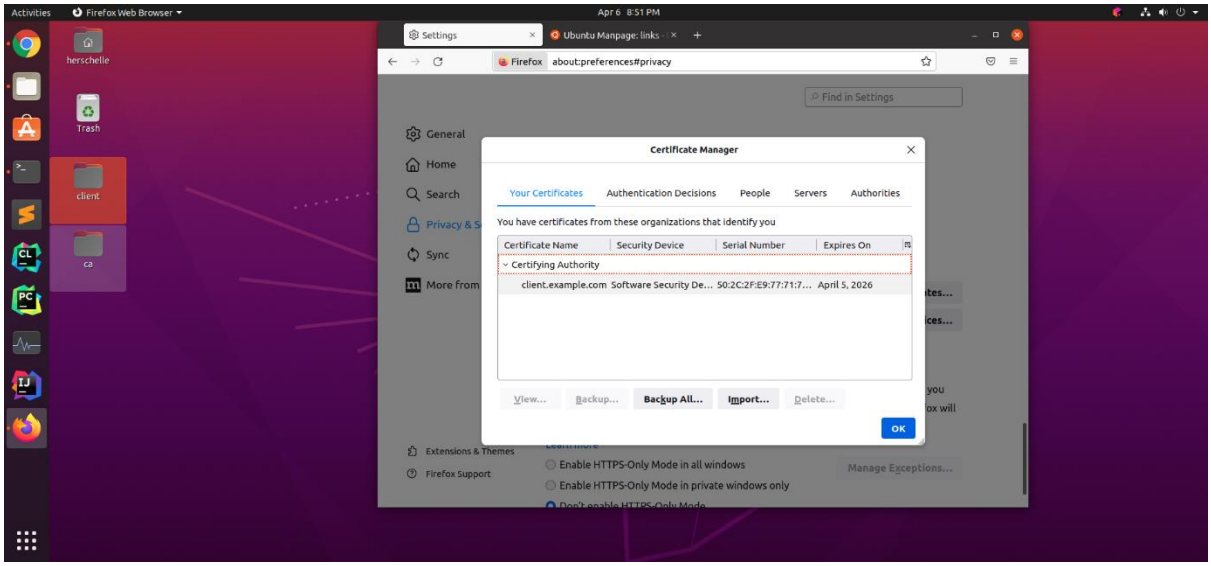
Before configuring the browser, we need to convert client certificate to pcks format as browsers accepts them in this format. This is done with the following command.

openssl pkcs12 -export -out client/client.p12 -inkey client/client_key.pem -in client/client_cert.pem

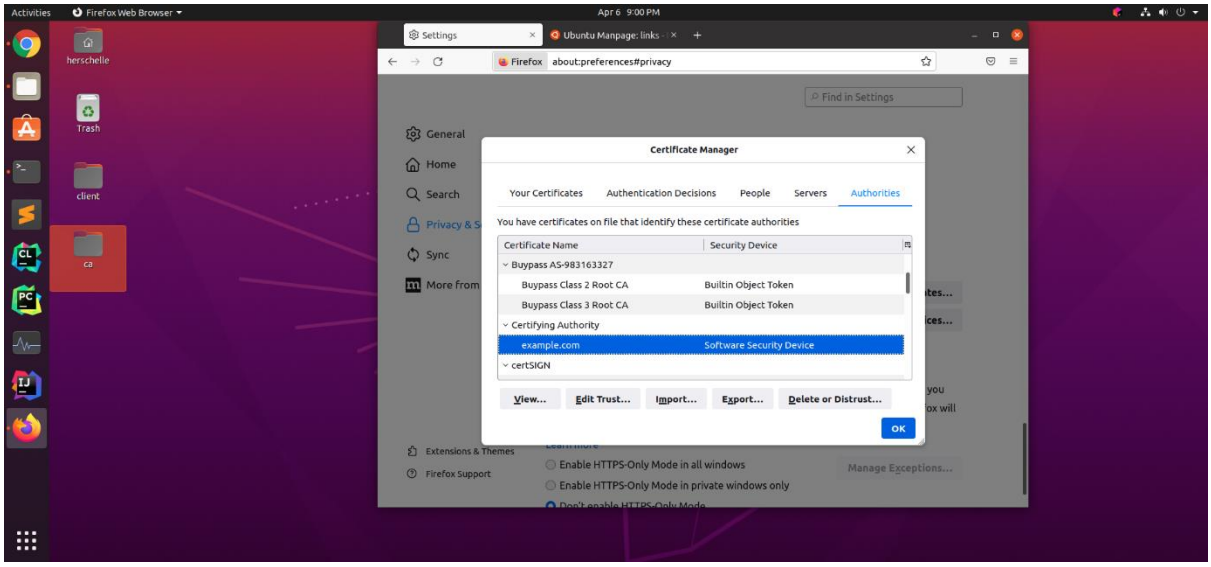
We see client.p12 file is generated which is ready to be imported to browser.



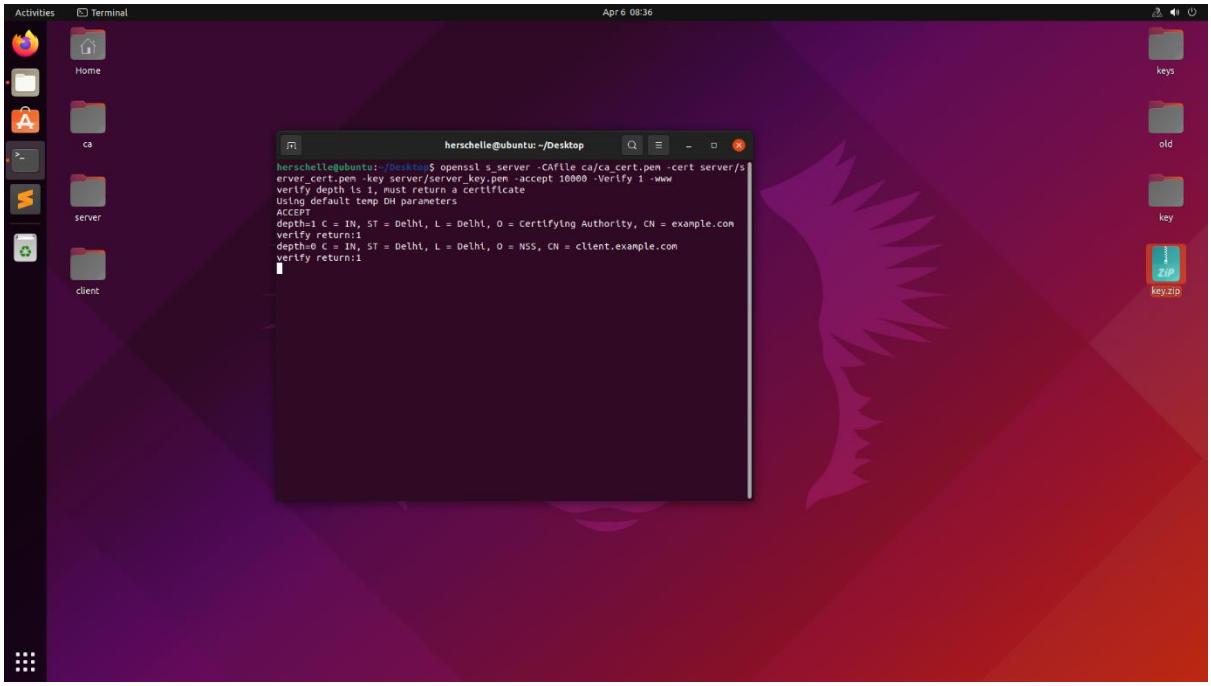
In the firefox settings we go to privacy and security tab and scroll down. Here we find view cerficates and go to “Your Certificate” tab and import the client.p12 file.



Then we go to Authorities tab and import the file ca_cert.pem in ca folder.

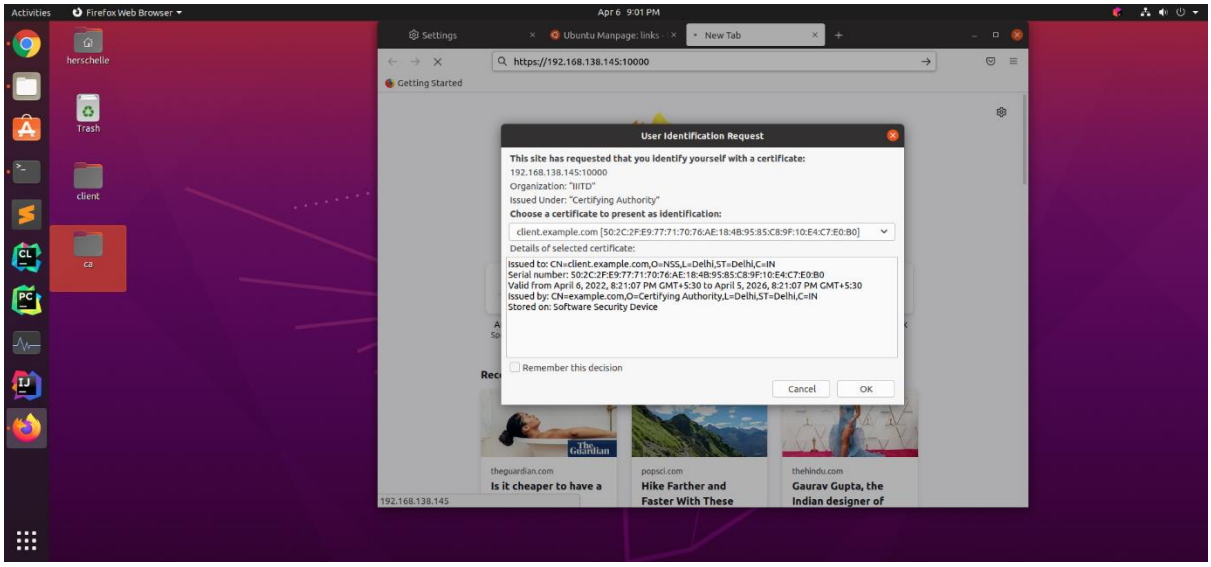


Now we run the s_server with -www option and connect to this server via our configured browser on second vm.

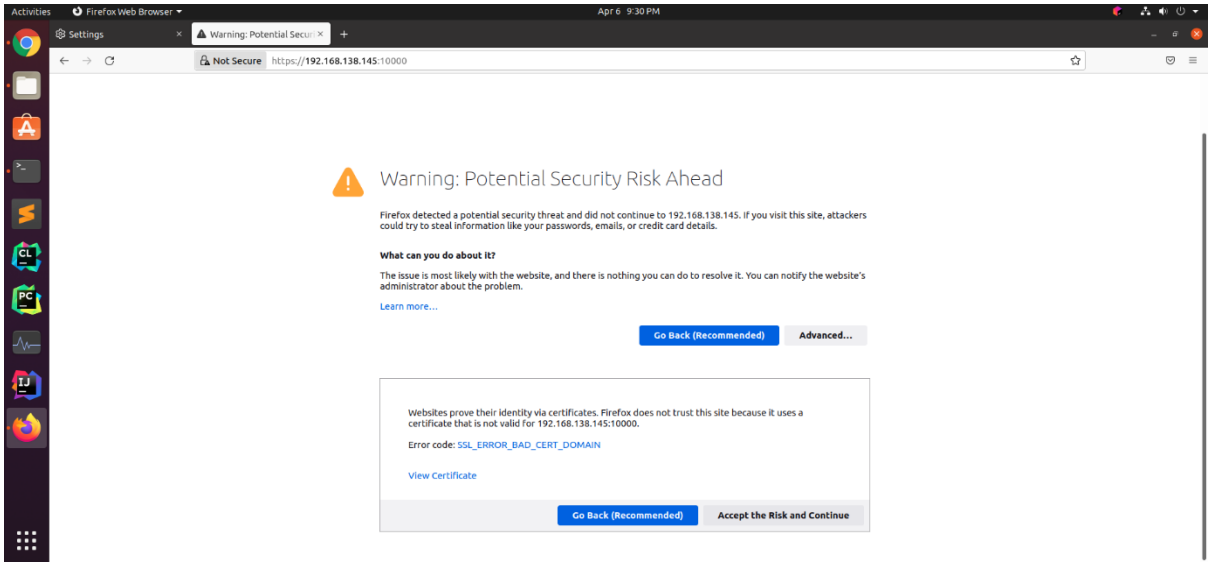


Ip of vm running s_server in my case is 192.168.138.145, we enter the following url in the browser-

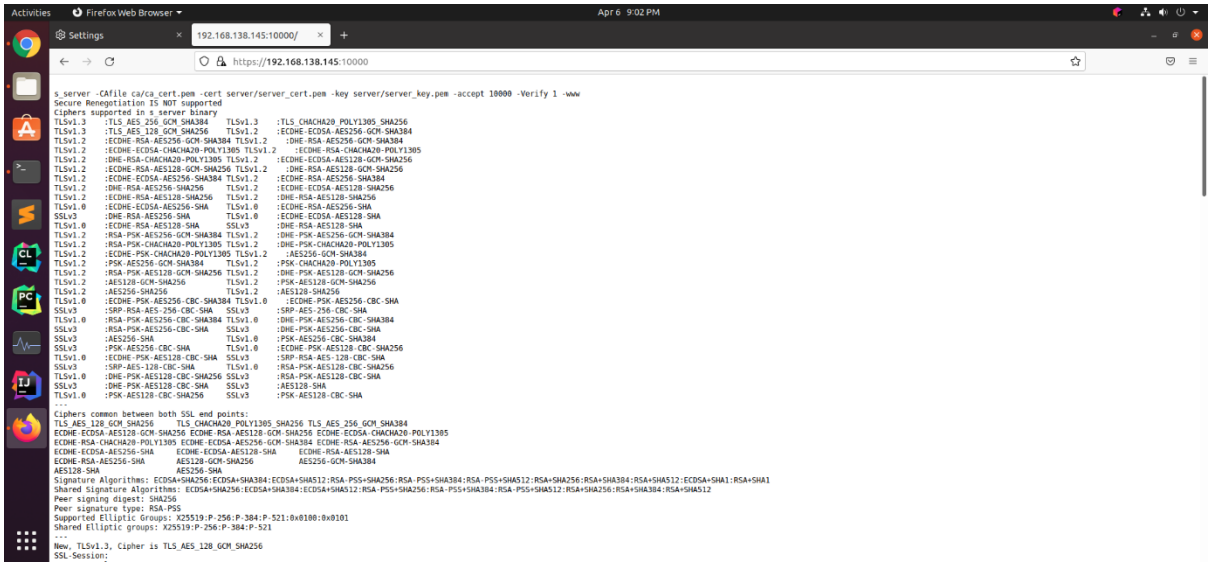
https://192.168.138.145:10000 and it asks for a certificate as s_server is in verify mode. Browser correctly identifies the client certificate and we proceed.



Note that the below warning is domain error and not some certificate error because we set the certificate uploaded as trusted certificate. We entered example.com as domain which we don't own so the following error. And click accept risk and continue.

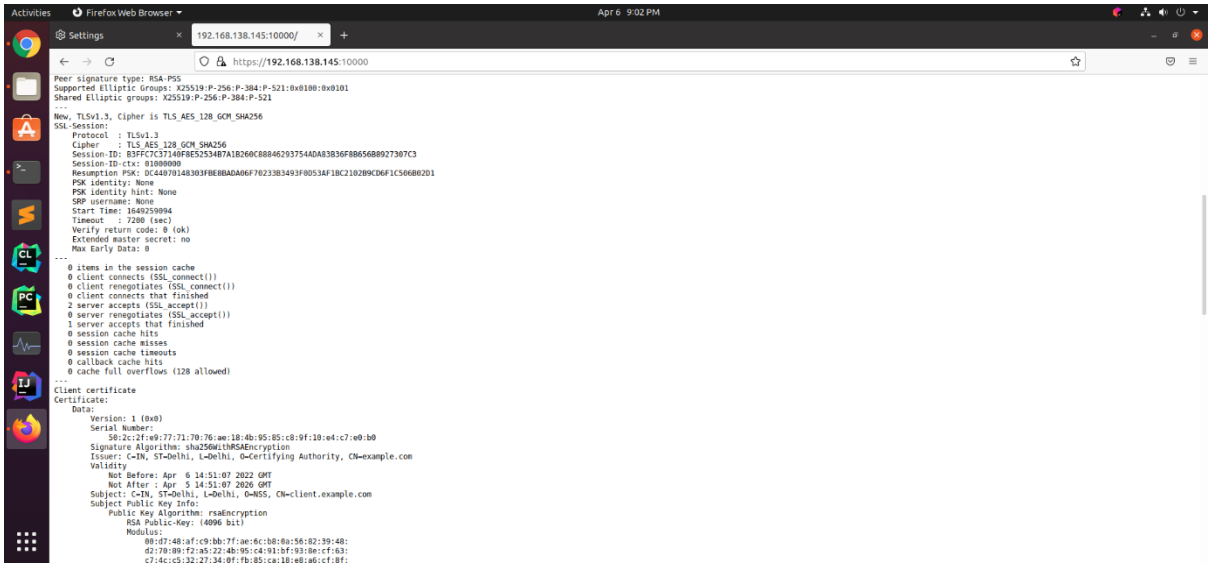


We receive the following response


Activities
Firefox Web Browser
Apr 6 9:02 PM
Settings
192.168.138.145:10000/
https://192.168.138.145:10000
s_server -CAfile ca/ca_cert.pem -cert server/server_cert.pem -key server/server_key.pem -accept 10000 -Verify 1 -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

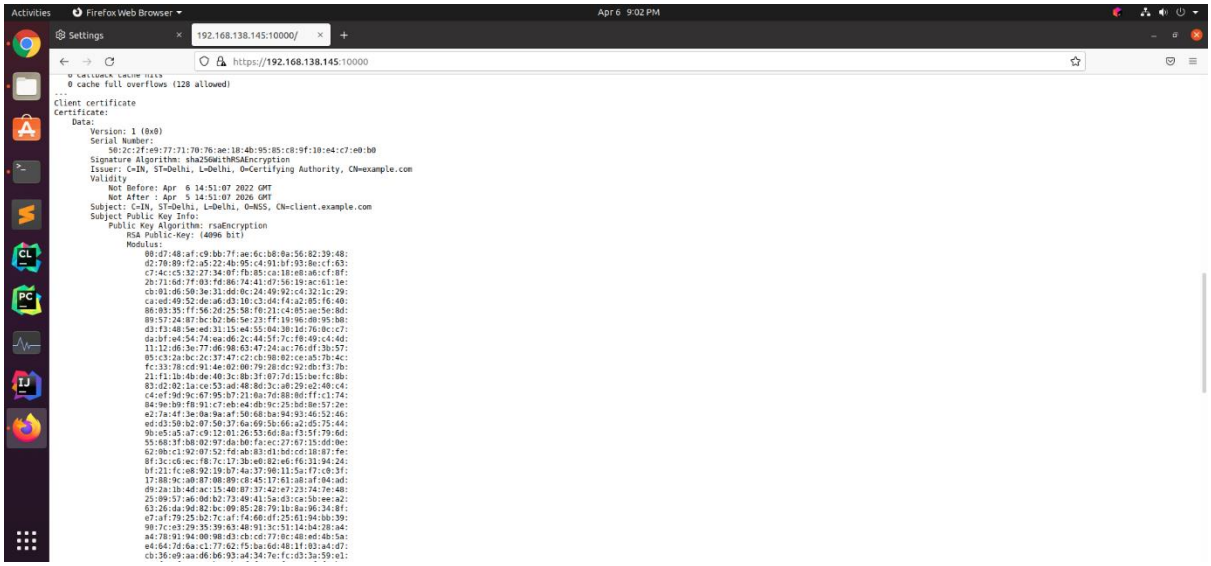
Ciphers common between both SSL end points:
TLS_AES_128_GCM_SHA256 TLS_CHACHA20_POLY1305_SHA256 TLS_AES_256_GCM_SHA384
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-CHACHA20-POLY1305
ECDHE-RSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-SHA 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
Peer signing digest: SHA256
Peer signature type: RSA-PSS
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:

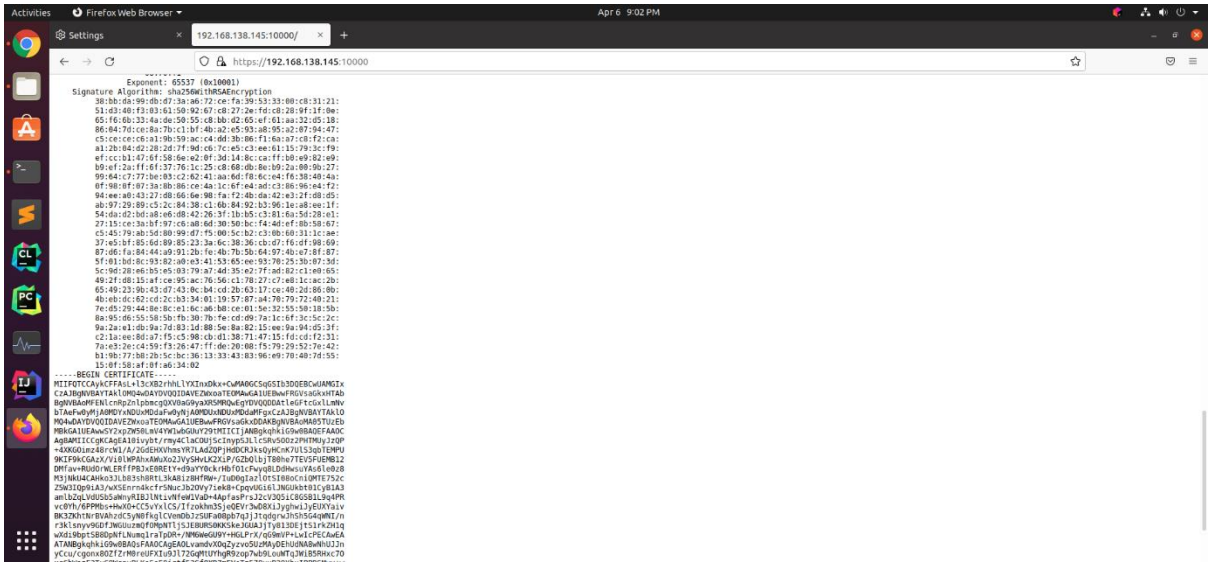

Activities
Firefox Web Browser
Apr 6 9:02 PM
Settings
192.168.138.145:10000/
https://192.168.138.145:10000
Peer signature type: RSA-PSS
Supported Elliptic Groups: X25519:P-256:P-384:P-521:0x0100:0x0101
Shared Elliptic groups: X25519:P-256:P-384:P-521

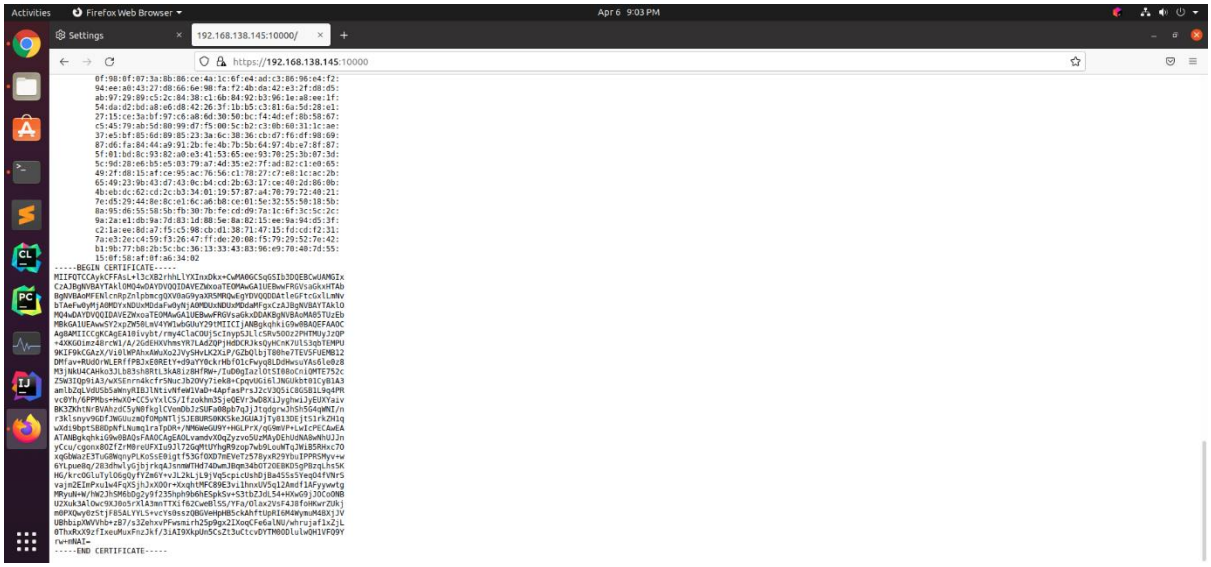
New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_128_GCM_SHA256
Session-ID: B3FFC7C37140F8E52534B7A1B260C88846293754ADA83B36F8B656B8927307C3
Session-ID-ctx: 01000000
Resumption PSK: DC44070148303FBEBBADA06F70233B3493F80534F1BC2102B9CD6F1C506B02D1
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1649259094
Timeout : 7200 (sec)
Verify return code: 0 (ok)
Extended master secret: no
Max Early Data: 0
---
0 items in the session cache
0 client connects (SSL_connect())
0 client renegotiates (SSL_connect())
0 client connects that finished
2 server accepts (SSL_accept())
0 server renegotiates (SSL_accept())
1 server accepts that finished
0 session cache hits
0 session cache misses
0 session cache timeouts
0 callback cache hits
0 cache full overflows (128 allowed)

Client certificate
Certificate:
Data:
Version: 1 (0x0)
Serial Number:
50:2c:2f:e9:77:71:70:76:ae:18:4b:95:85:c8:9f:10:e4:c7:e0:b0
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=IN, ST=Delhi, L=Delhi, O=Certifying Authority, CN=example.com
Validity
Not Before: Apr 6 14:51:07 2022 GMT
Not After : Apr 5 14:51:07 2026 GMT
Subject: C=IN, ST=Delhi, L=Delhi, O=NSS, CN=client.example.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (4096 bit)
Modulus:
00:d7:48:af:c9:bb:7f:ae:6c:b8:0a:56:82:39:48:
d2:70:89:f2:a5:22:4b:95:c4:91:bf:93:8e:cf:63:
c7:4c:c5:32:27:34:0f:fb:85:ca:18:e8:a6:cf:8f:


Activities
Firefox Web Browser
Apr 6 9:02 PM
Settings
192.168.138.145:10000/
https://192.168.138.145:10000
0 cache full overflows (128 allowed)

Client certificate
Certificate:
Data:
Version: 1 (0x0)
Serial Number:
50:2c:2f:e9:77:71:70:76:ae:18:4b:95:85:c8:9f:10:e4:c7:e0:b0
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=IN, ST=Delhi, L=Delhi, O=Certifying Authority, CN=example.com
Validity
Not Before: Apr 6 14:51:07 2022 GMT
Not After : Apr 5 14:51:07 2026 GMT
Subject: C=IN, ST=Delhi, L=Delhi, O=NSS, CN=client.example.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (4096 bit)
Modulus:
00:d7:48:af:c9:bb:7f:ae:6c:b8:0a:56:82:39:48:
d2:70:89:f2:a5:22:4b:95:c4:91:bf:93:8e:cf:63:
c7:4c:c5:32:27:34:0f:fb:85:ca:18:e8:a6:cf:8f:
2b:71:dd:7f:03:fd:86:7a:41:d7:56:19:ac:61:1e:
cb:01:d6:50:3e:31:dd:0c:24:49:92:c4:32:1c:29:
ca:ed:49:52:de:a6:d3:10:c3:d4:f4:a2:05:f6:40:
88:83:35:ff:56:2d:25:58:f6:21:c4:85:ae:5e:8d:
89:57:24:87:bc:b2:b6:5e:23:ff:19:96:d0:95:b8:
d3:f3:48:5e:ed:31:15:e4:55:04:30:1d:76:0c:c7:
da:bf:e4:54:74:ea:d6:2c:44:5f:7c:f0:49:c4:4d:
11:12:d6:3e:77:d6:98:63:47:24:ac:76:df:3b:57:
05:c3:2a:bc:2c:37:47:c2:cb:98:02:ce:a5:7b:4c:
fc:33:78:cd:91:4e:02:00:79:28:dc:92:dc:f3:7b:
21:f1:1b:4b:de:40:3c:8b:3f:07:7d:15:be:fc:8b:
83:d2:02:1a:ce:53:ad:48:8d:3c:a0:29:e2:40:c4:
c4:ef:9d:9c:67:95:b7:21:0a:7d:88:0d:ff:c1:74:
84:9e:b9:f8:91:c7:eb:e4:db:9c:25:bd:8e:57:2e:
e2:7a:4f:3e:0a:9a:af:50:68:ba:94:93:46:52:46:
ed:d3:50:b2:07:50:37:6a:69:5b:66:a2:d5:75:44:
9b:e5:a5:a7:c9:12:01:26:53:6d:8a:f3:5f:79:6d:
55:68:3f:b8:02:97:da:b0:fa:ec:27:87:15:dd:0e:
62:0b:c1:92:07:52:fd:ab:83:d1:bd:cd:10:87:fe:
8f:3c:c6:ec:f8:7c:17:3b:e0:82:e6:f6:31:94:24:
bf:21:fc:e8:92:19:b7:4a:37:90:11:5a:f7:c0:3f:
17:88:9c:a0:87:00:89:c8:45:17:61:a8:af:04:ad:
d9:2a:1b:4d:ac:15:40:87:37:42:e7:23:74:7e:48:
25:09:57:a6:0d:b2:73:49:41:5a:d3:ca:5b:ee:a2:
63:26:da:9d:82:bc:09:85:28:79:1b:8a:96:34:8f:
e7:af:79:25:b2:7c:af:f4:60:df:25:61:94:bb:39:
98:7c:e3:29:35:39:63:4b:91:3c:51:14:b4:28:a4:
a4:78:91:94:00:98:d3:cb:cd:77:8c:48:ed:4b:5a:
e4:64:7d:6a:c1:77:62:f5:ba:6d:48:1f:03:a4:d7:
cb:36:e9:aa:d6:b6:93:a4:34:7e:fc:d3:3a:59:e1:





Task 2:

Ref: http://kb.ictbanking.net/article.php?id=706

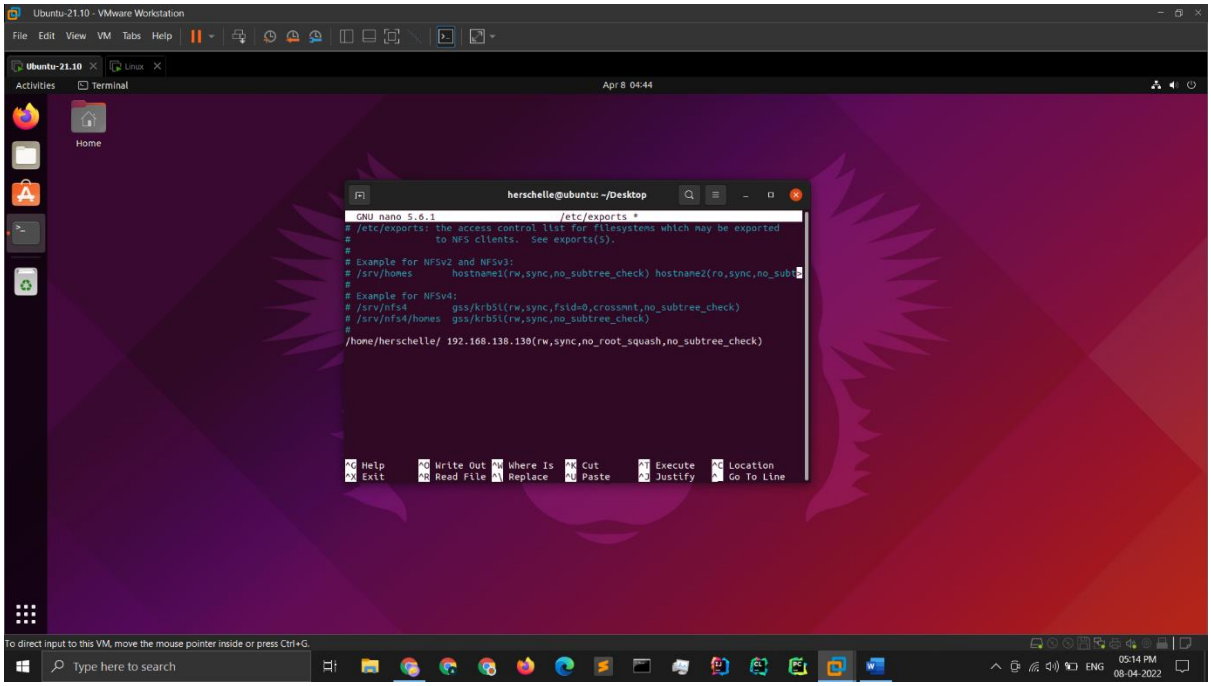
My Server VM IP: 192.168.138.145; Name of VM: Ubuntu 21.10

My Client VM IP: 192.168.138.130; Name of VM: Linux

Configuring Server VM

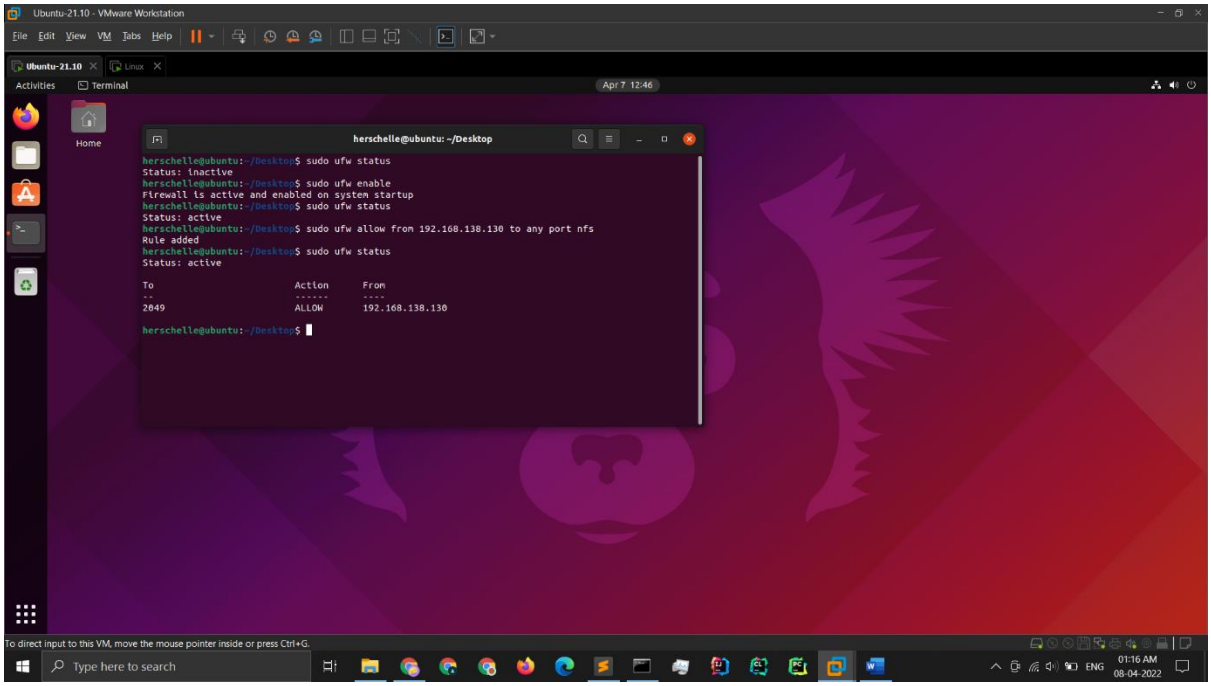
sudo apt install nfs-kernel-server

Edit the /etc/exports file as shown below, to export the home directory which in my case is "/home/herschelle"



Now restart the nfs server with “sudo systemctl restart nfs-kernel-server”

If your firewall is disabled do enable with “sudo ufw enable” and allow connection from client as done below.



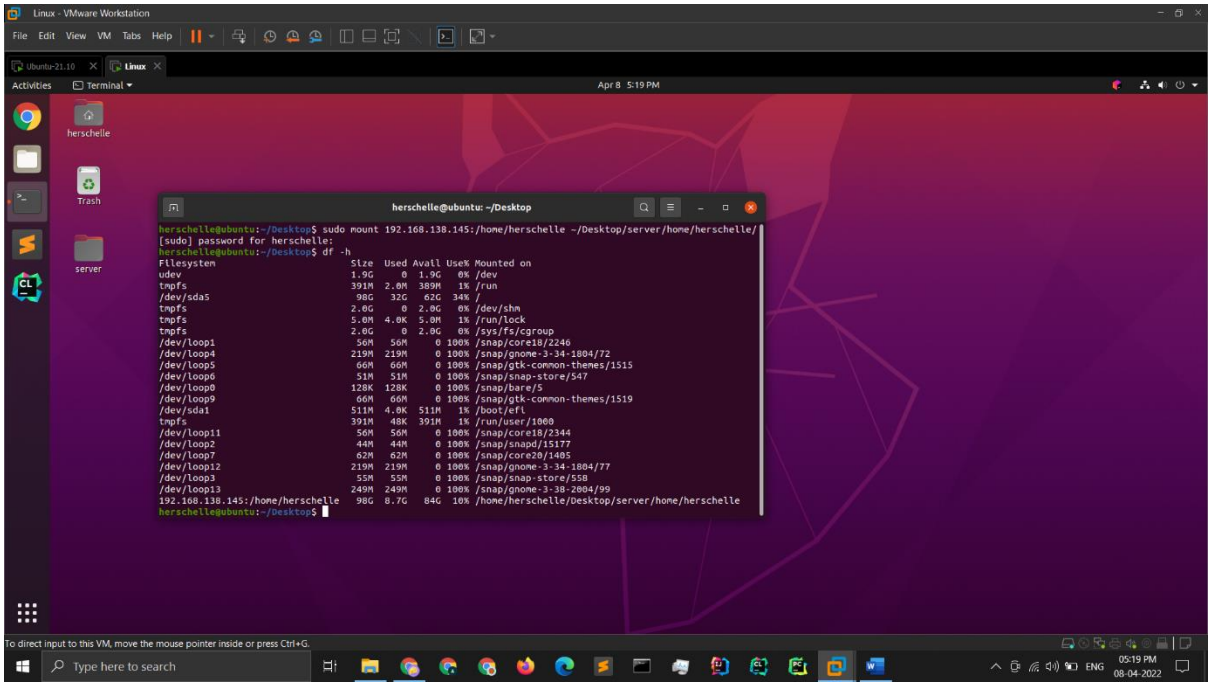
Configuring client:

sudo apt install nfs-common

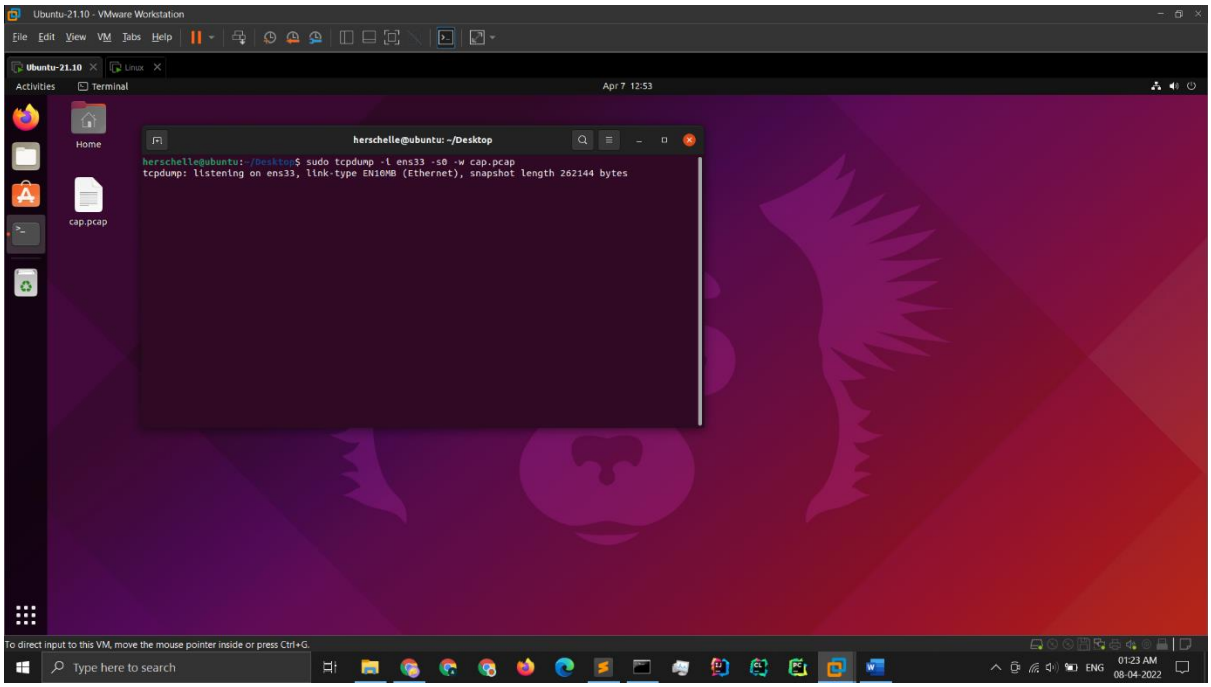
Mount the desktop with the command shown below.

I created a folder on desktop as server/home/herschelle which will act as home directory of the client.

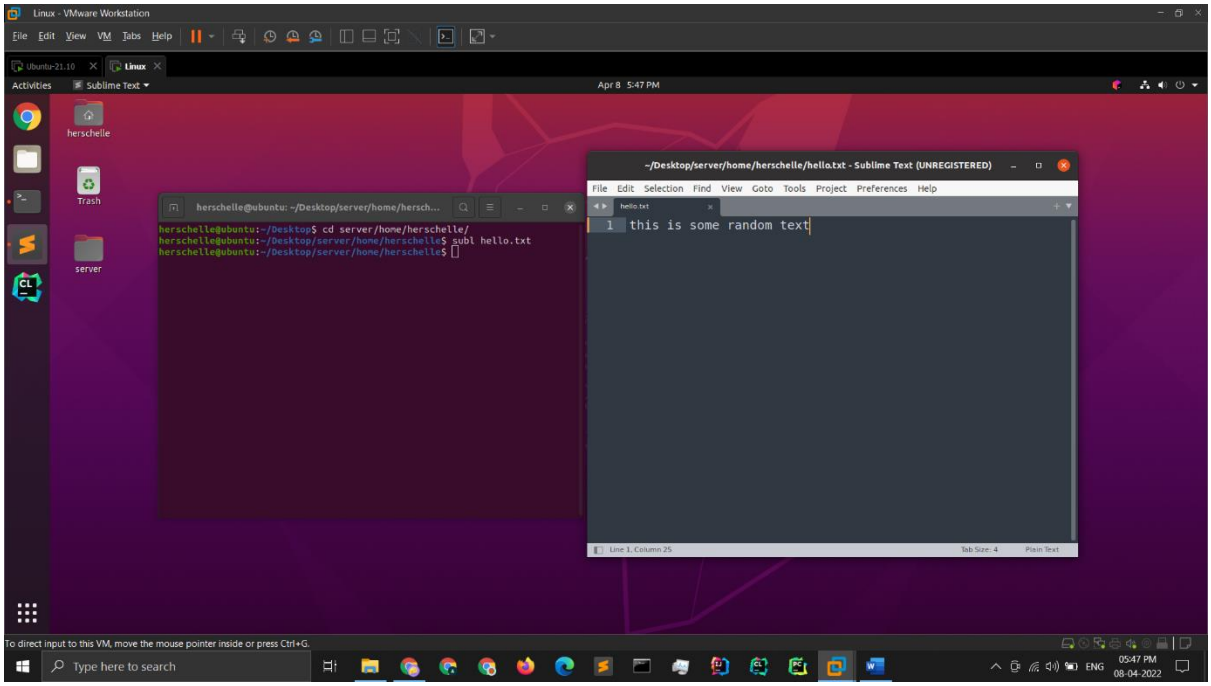
We can see the mounted drive with “df -h”.



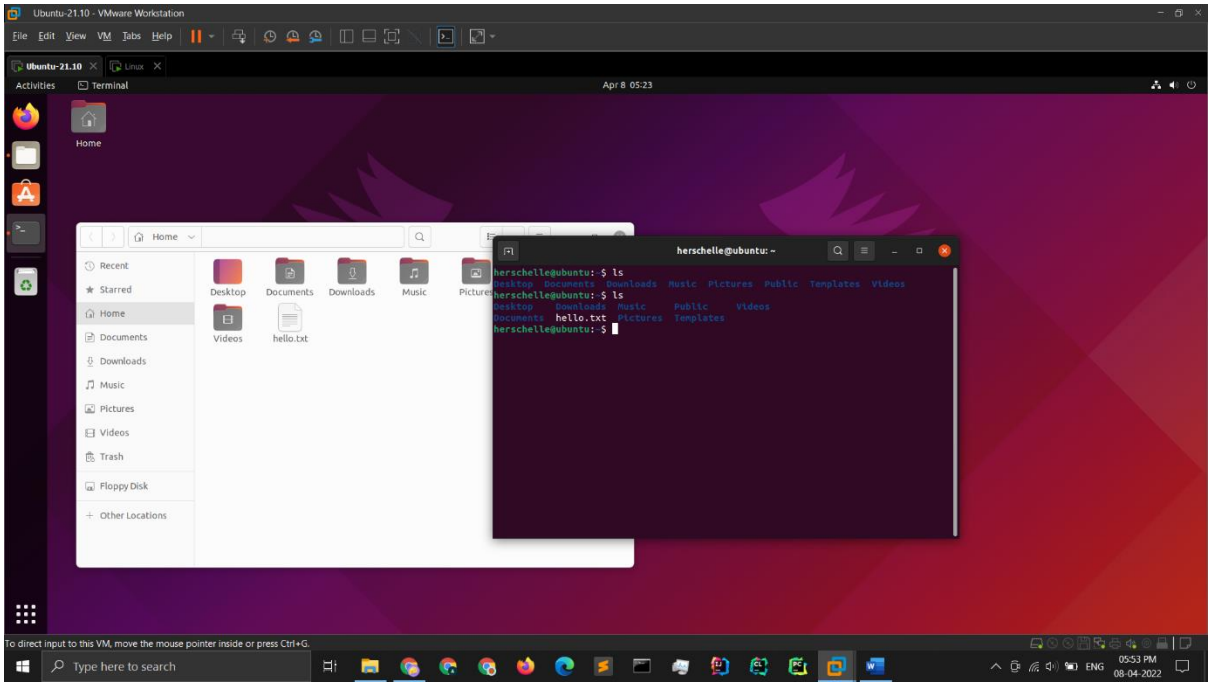
Go back to server and start capturing packets



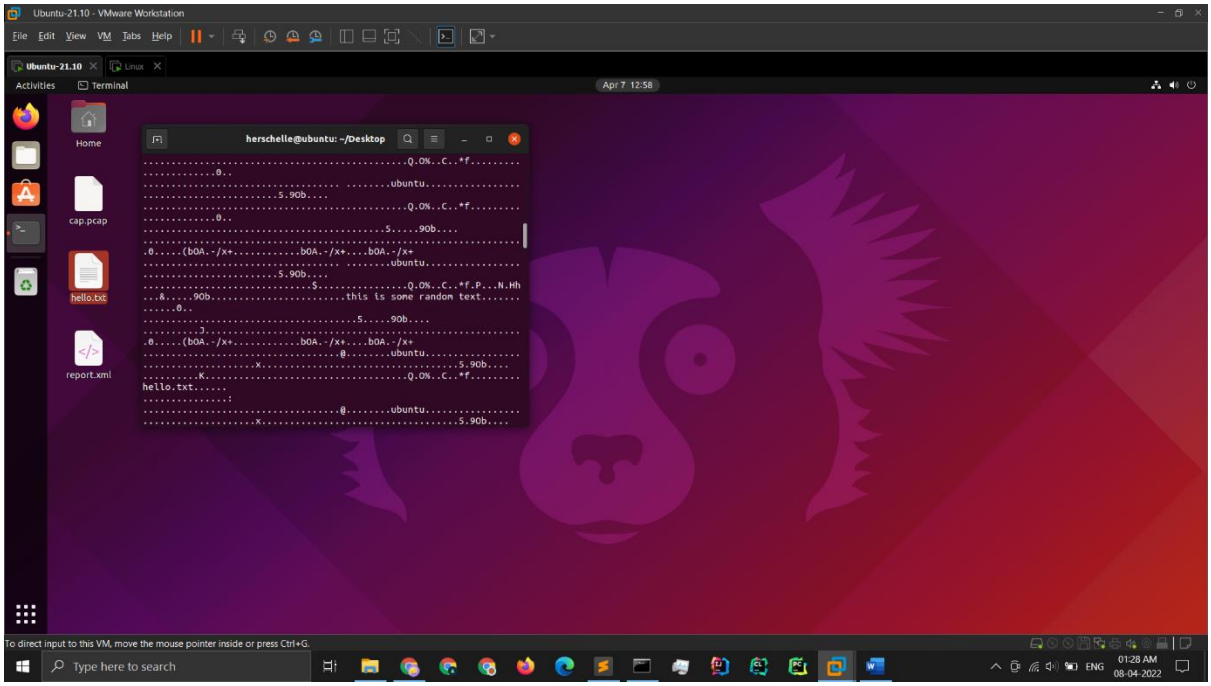
Now on client we create a file on client and add some text



And the data arrives at home directory of the server.



Analyse the captured packets.

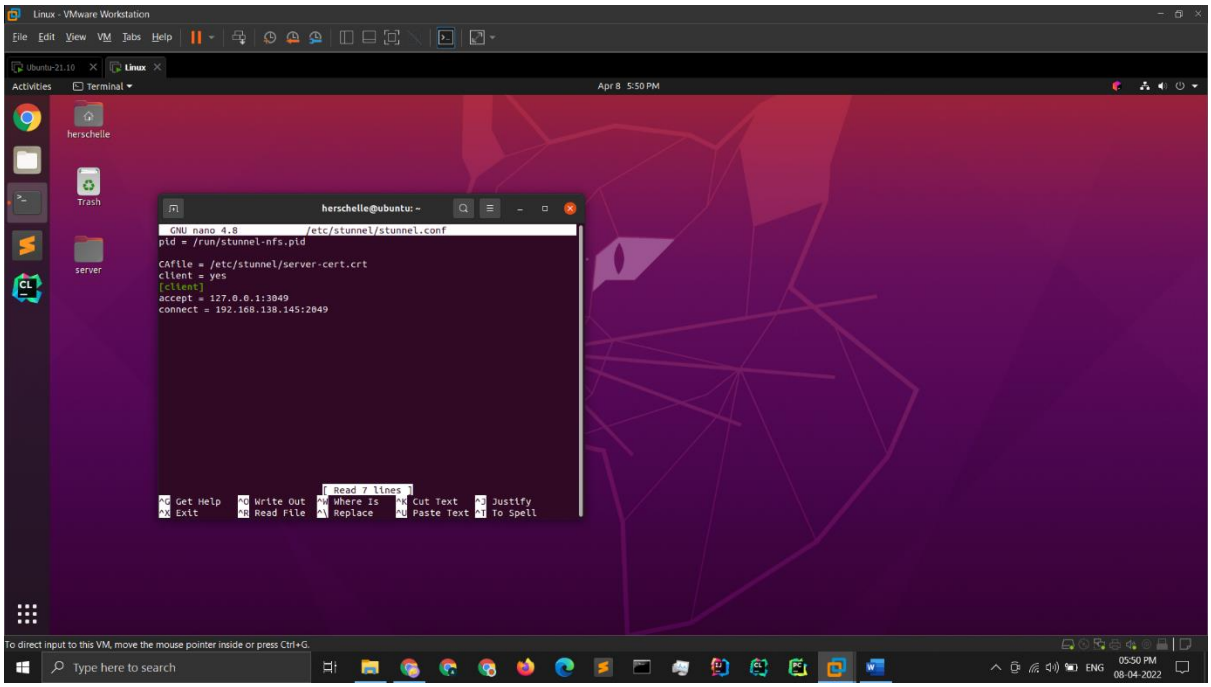


We can see packets carry data in plain text which is already knew from the question.

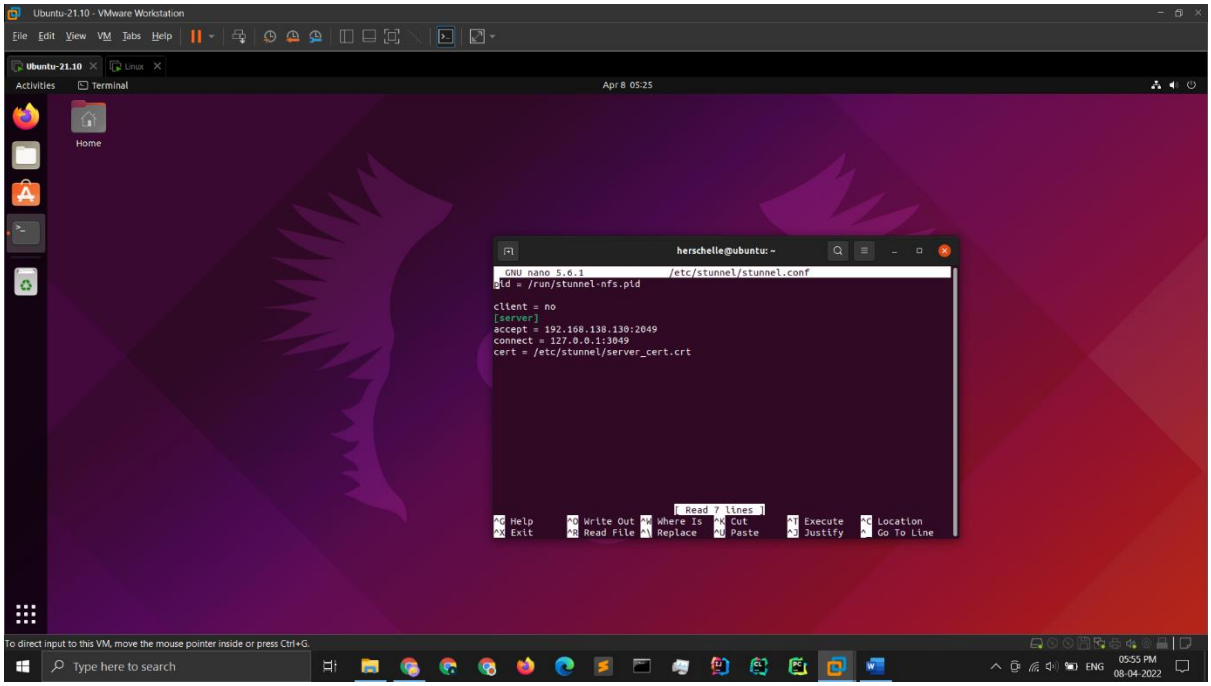
Now we install stunnel on both server and client with “sudo apt-get install stunnel4”

Create server certificate and key and place them in /etc/stunnel of both the client and server.

On client create a file in /etc/stunnel and name it stunnel.conf and write the text in it as shown below.



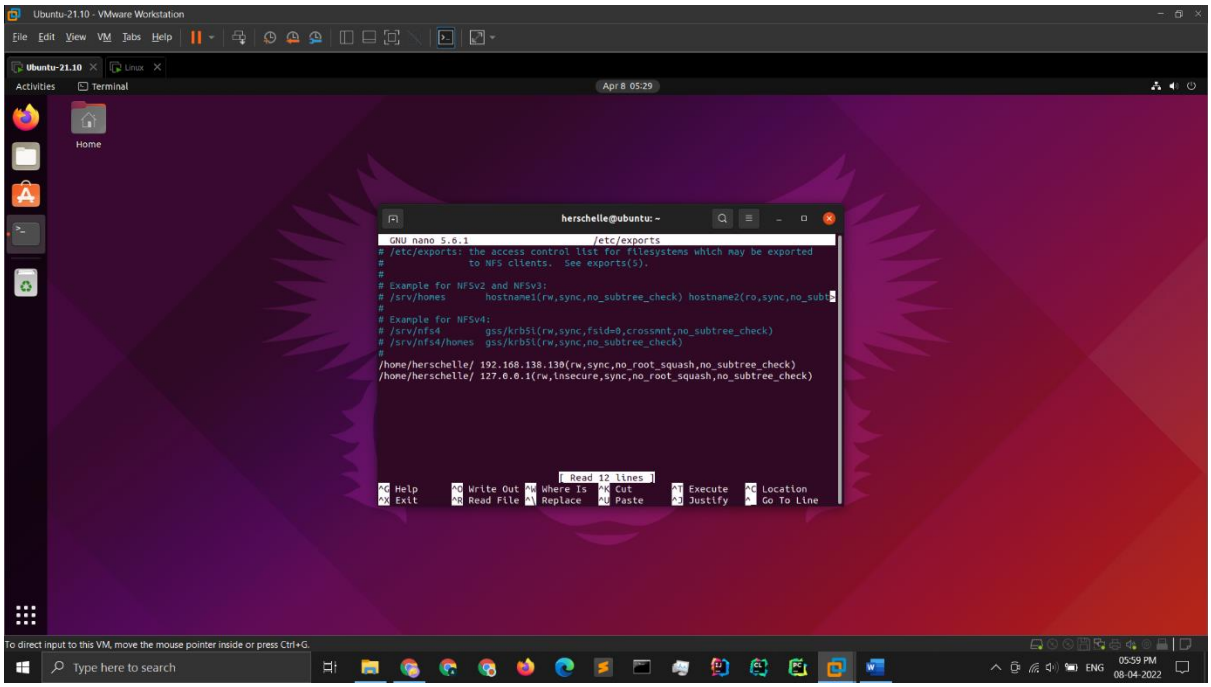
For server again do the same process but add the following text



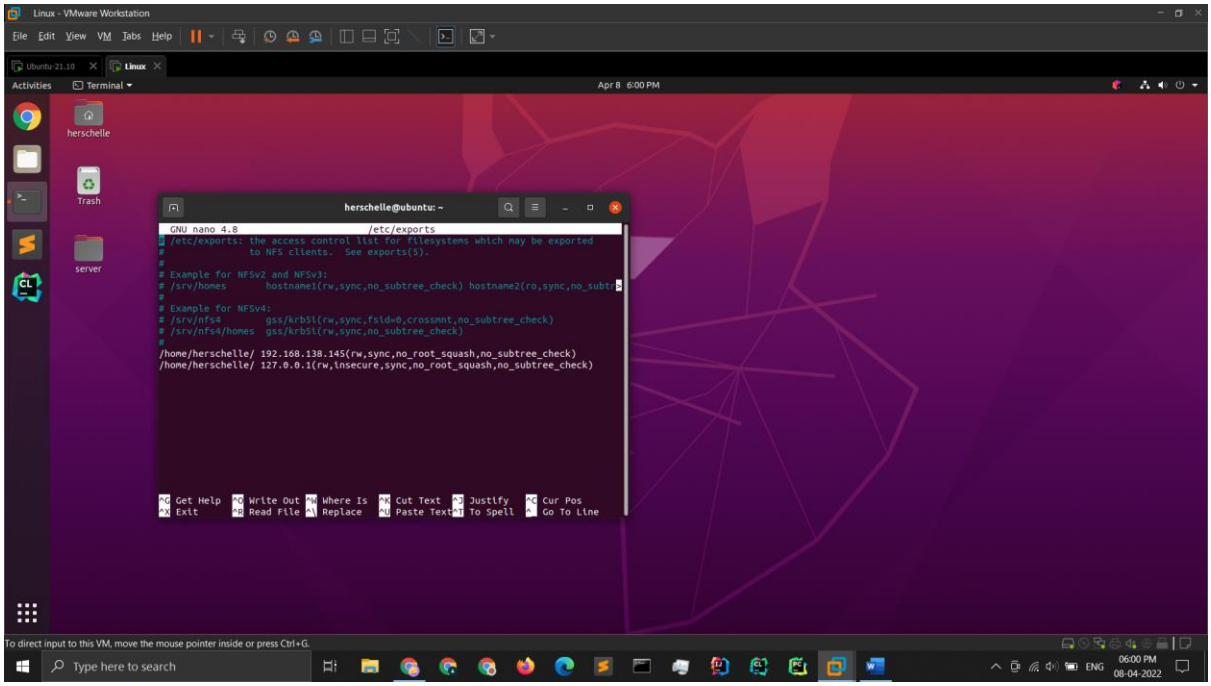
Now restart the stunnel service on both server and client with “sudo systemctl restart stunnel4.service”

Modify the /etc/stunnel/stunnel.conf files of server and client to configure stunnel as shown below.

On server:

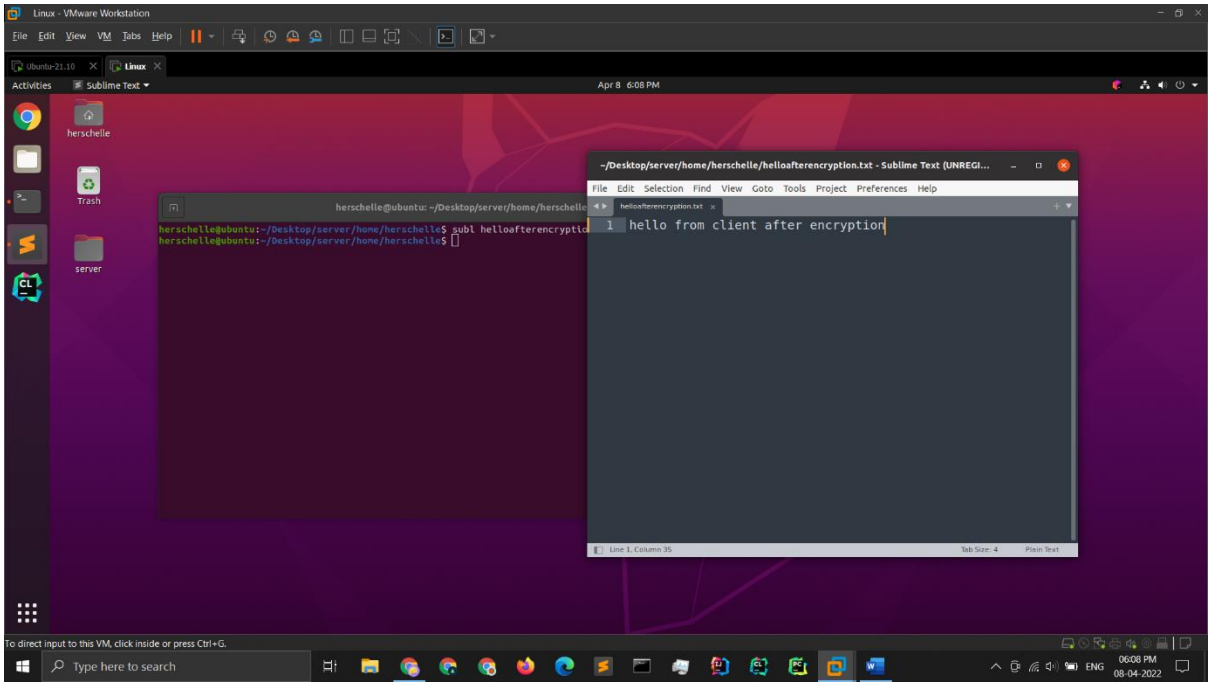


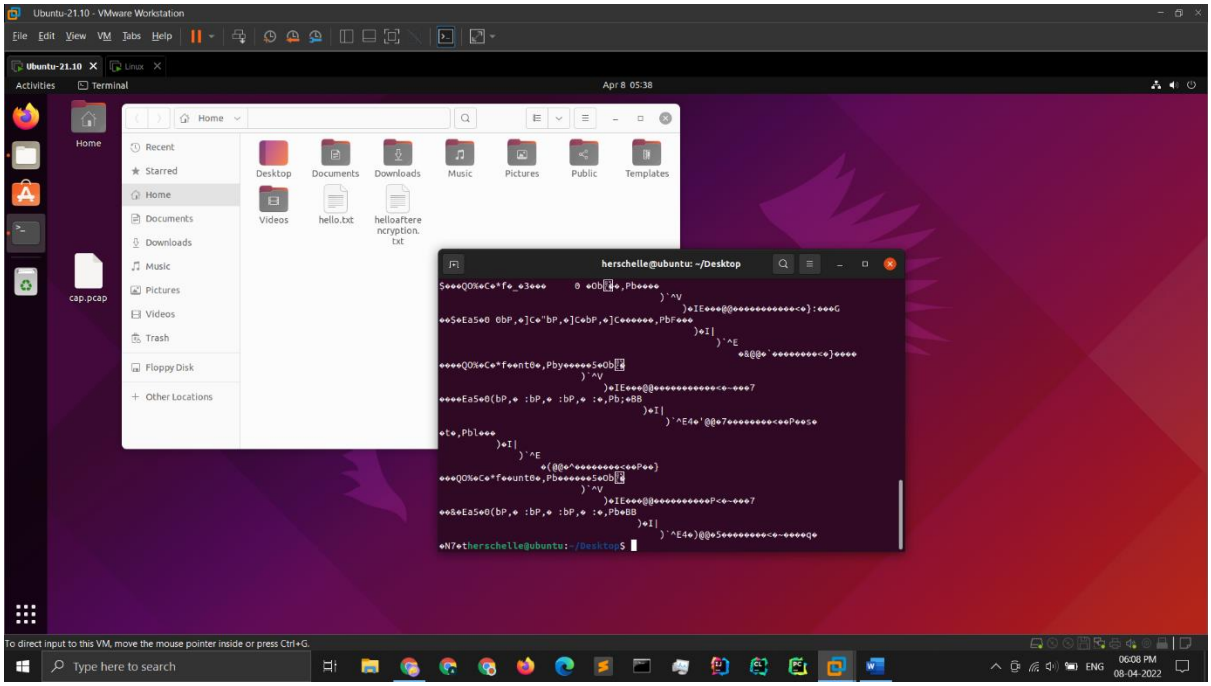
On client:



Mount the home directory of the server this time on localhost of the client with the command “sudo mount 127.0.0.1:3049:/home/herschelle ~/Desktop/server/home/herschelle/” where stunnel service is listening on port 3049 as configured in .conf files and it will forward the traffic to the server.

Restart the services (nfs and stunnel) and start capturing the packets and we see




Ubuntu-21.10 - VMware Workstation
File Edit View VM Tabs Help
Ubuntu-21.10
Linux
Activities
Terminal
Apr 8 05:38
Home
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
Floppy Disk
Other Locations
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
hello.txt
helloafterencryption.txt
cap.pcap
herschelle@ubuntu: ~/Desktop
herschelle@ubuntu:~/Desktop$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Type here to search
ENG
06:08 PM
08-04-2022