



الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

12th Project

Networks Security (CCY3201)

➤ TA: Eng. Abdelrhman solyman

Nada Ibrahim 221003011

Mawada Ayman 221003907

Lecturer: Dr. Ayman Adel

Course: Network Security

Part 1: TLS – HTTPS Web App Using OpenSSL

A) Generate Certificates Using OpenSSL

begin by setting up a Certificate Authority (CA), then generate and sign certificates for both client and server.

A. Create Root CA (on server VM)

The terminal window shows the following command being run:

```
mint@mint:~$ cd /etc/ssl/certs
mint@mint:~/etc/ssl/certs$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 365 -out rootCA.pem
```

Followed by the configuration of the certificate:

```
Country Name (2 letter code) [AU]:eg
State or Province Name (full name) [Some-State]:Alex
Locality Name (eg, city) []:Abiquiu
Organization Name (eg, company) [Internet Widgets Pty Ltd]:AAST
Organizational Unit Name (eg, section) []:AAST
Common Name (e.g. server FQDN or YOUR name) []:server.local
Email Address []:newdayman60@gmail.com
```

And finally the creation of the private key:

```
mint@mint:~/etc/ssl/certs$ openssl genpkey -out rootCA.key -aes256
```

B. Create Server Private Key and CSR

The terminal window shows the following command being run:

```
mint@mint:~$ cd /etc/ssl/certs
mint@mint:~/etc/ssl/certs$ openssl genrsa -out server.key 2048
```

Followed by the configuration of the certificate request:

```
Country Name (2 letter code) [AU]:eg
State or Province Name (full name) [Some-State]:Alex
Locality Name (eg, city) []:Abiquiu
Organization Name (eg, company) [Internet Widgets Pty Ltd]:AAST
Organizational Unit Name (eg, section) []:AAST
Common Name (e.g. server FQDN or YOUR name) []:server.local
Email Address []:newdayman60@gmail.com
```

And finally the creation of the certificate signing request (CSR):

```
mint@mint:~/etc/ssl/certs$ openssl req -new -key server.key -out server.csr
```

C. Sign Server Certificate with Root CA

```
Linux Mint Server - VMware Workstation
File Edit View Search Terminal Help
Email Address []:mawadaayman663@gmail.com
mint@mint:~/cas openssl genrsa -out server.key 2048
mint@mint:~/cas openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
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]:eg
State or Province Name (full name) [Some-State]:Alex
Locality Name (eg, city) []:Abouqir
Organization Name (eg, company) [Internet Widgets Pty Ltd]:AAST
Organizational Unit Name (eg, section) []:AAST
Common Name (e.g. server FQDN or YOUR name) []:server.local
Email Address []:mawadaayman663@gmail.com

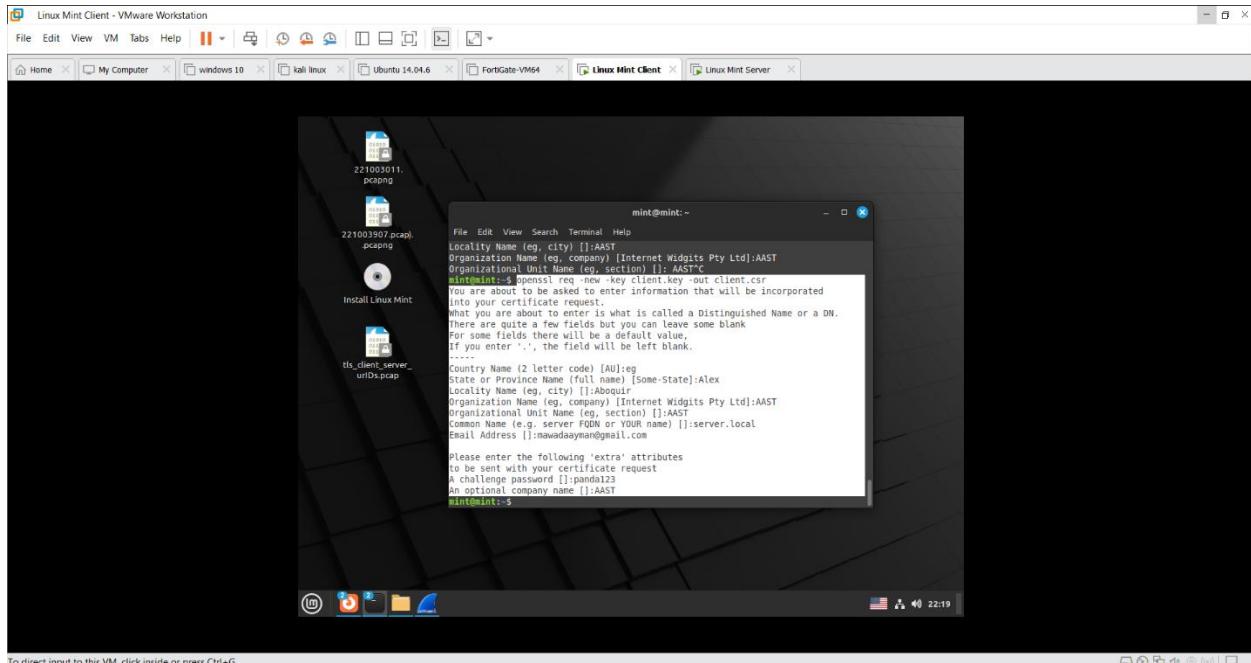
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:panda123
An optional company name []:cyber
mint@mint:~/cas openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out server.crt -days 365 -signer rootCA.pem
Certificate request self-signature ok
subjectC = eg, ST = Alex, L = Abouqir, O = AAST, OU = AAST, CN = server.local, emailAddress = mawadaayman663@gmail.com
mint@mint:~/cas openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out server.crt -days 365 -signer rootCA.pem
has256
Certificate request self-signature ok
subjectC = eg, ST = Alex, L = Abouqir, O = AAST, OU = AAST, CN = server.local, emailAddress = mawadaayman663@gmail.com
mint@mint:~/cas ls
rootCA.key rootCA.pem server.csr server.key
mint@mint:~/cas openssl x509 -req -in server.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out server.crt -days 365 -signer rootCA.pem
mint@mint:~/cas find -ca_name *.srl*
mint@mint:~/cas nano https.server.py
mint@mint:~/cas cp ./ca/server.crt ~/https_server.py
Sunday, May 25, 2025
23:45
```

D. for Client Certificate

Generate client key and CSR

```
Linux Mint Client - VMware Workstation
File Edit View Search Terminal Help
SSLKEYLOGFILE=/home/mint/.mozilla/firefox/221005011.pspng
mint@mint:~$ openssl genrsa -out client.key 2048
mint@mint:~$ openssl req -new -key client.key -out client.csr
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]:eg
State or Province Name (full name) [Some-State]:Alex
Locality Name (eg, city) []:Abouqir
Organization Name (eg, company) [Internet Widgets Pty Ltd]:AAST
Organizational Unit Name (eg, section) []:AAST
mint@mint:~$ openssl req -new -key client.key -out client.csr
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]:eg
```

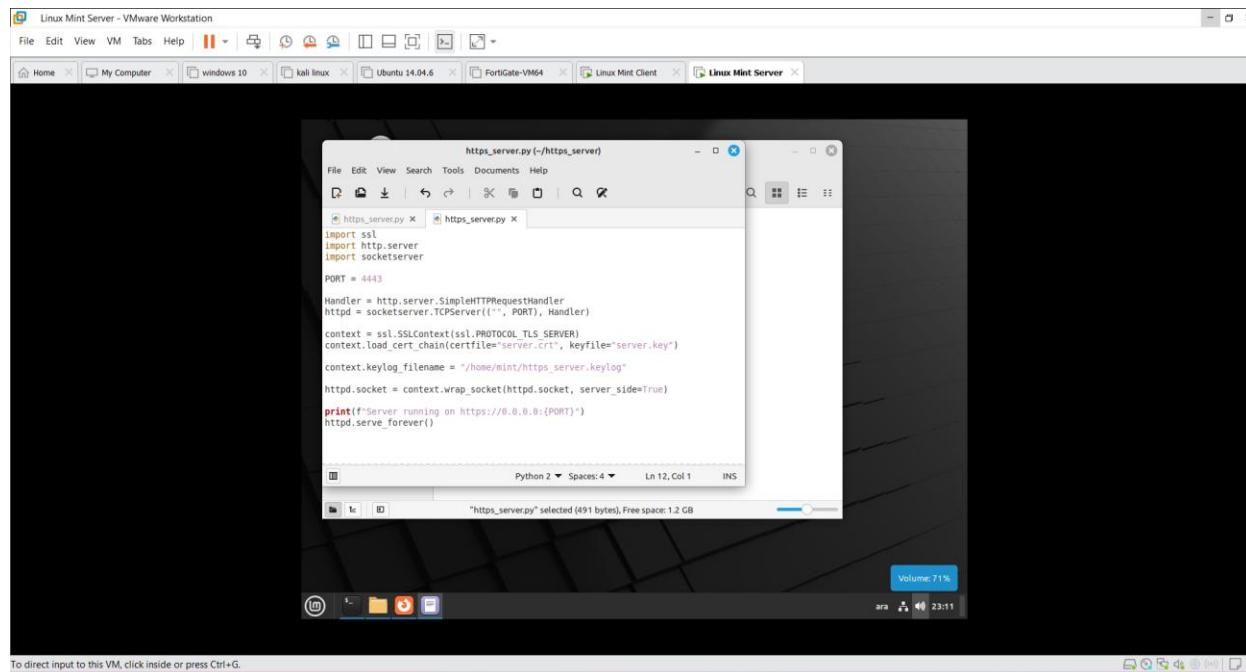
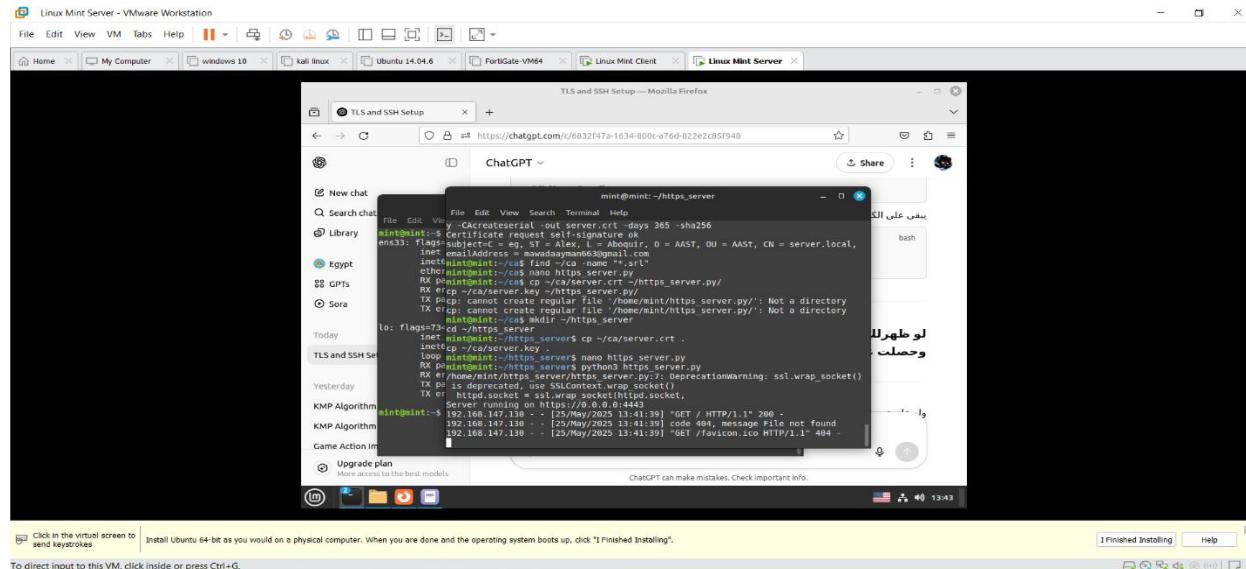
Sign client certificate with the same root CA



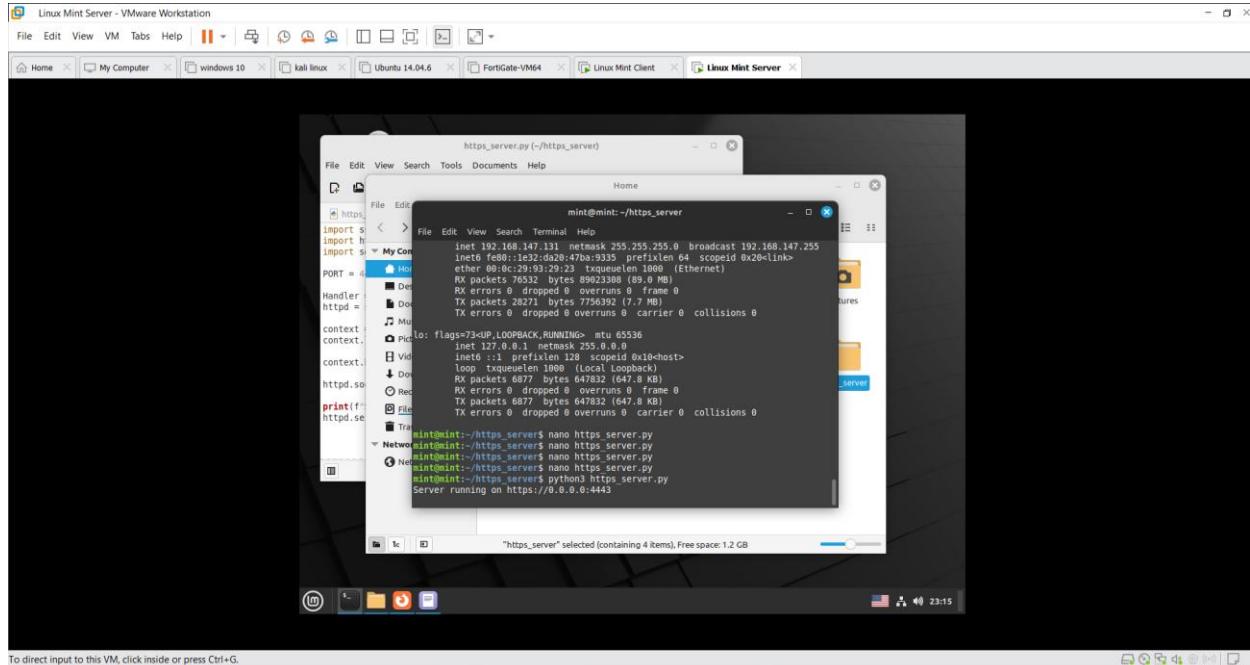
B)Simple TLS Client-Server App Server (Linux Mint Server)

Step 1: Create the HTTPS server script

nano https_server.py

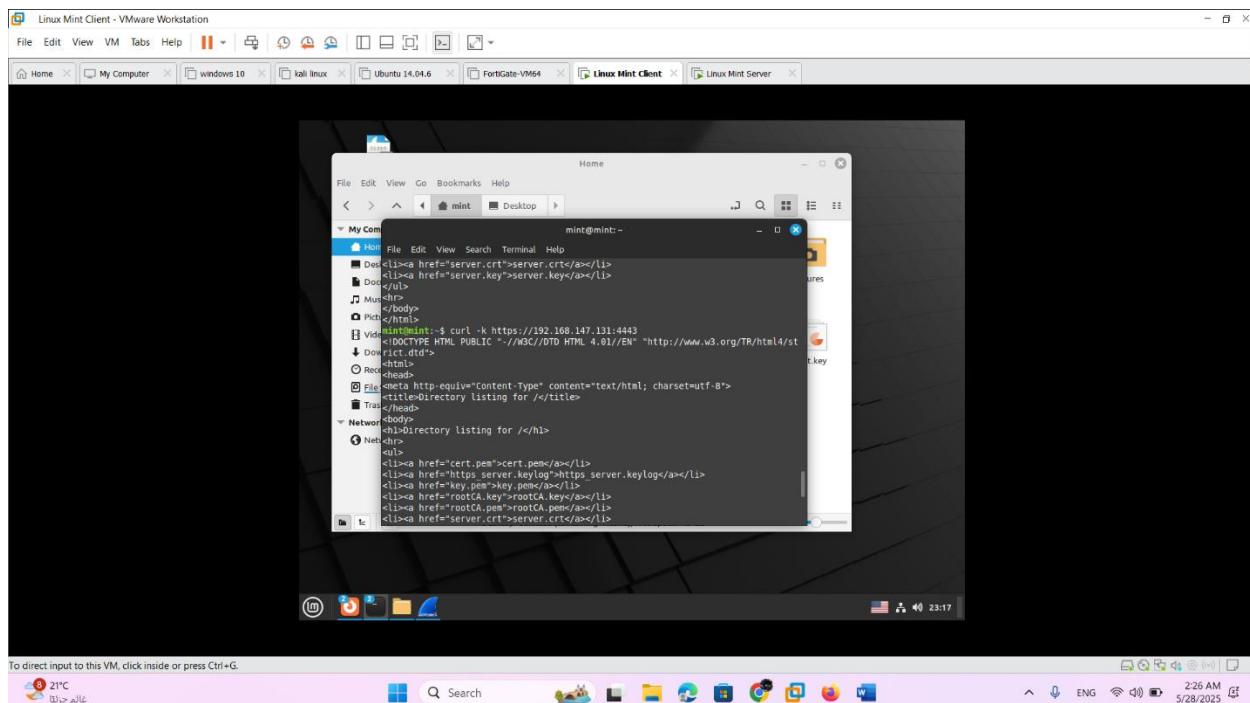


Step : Run the server

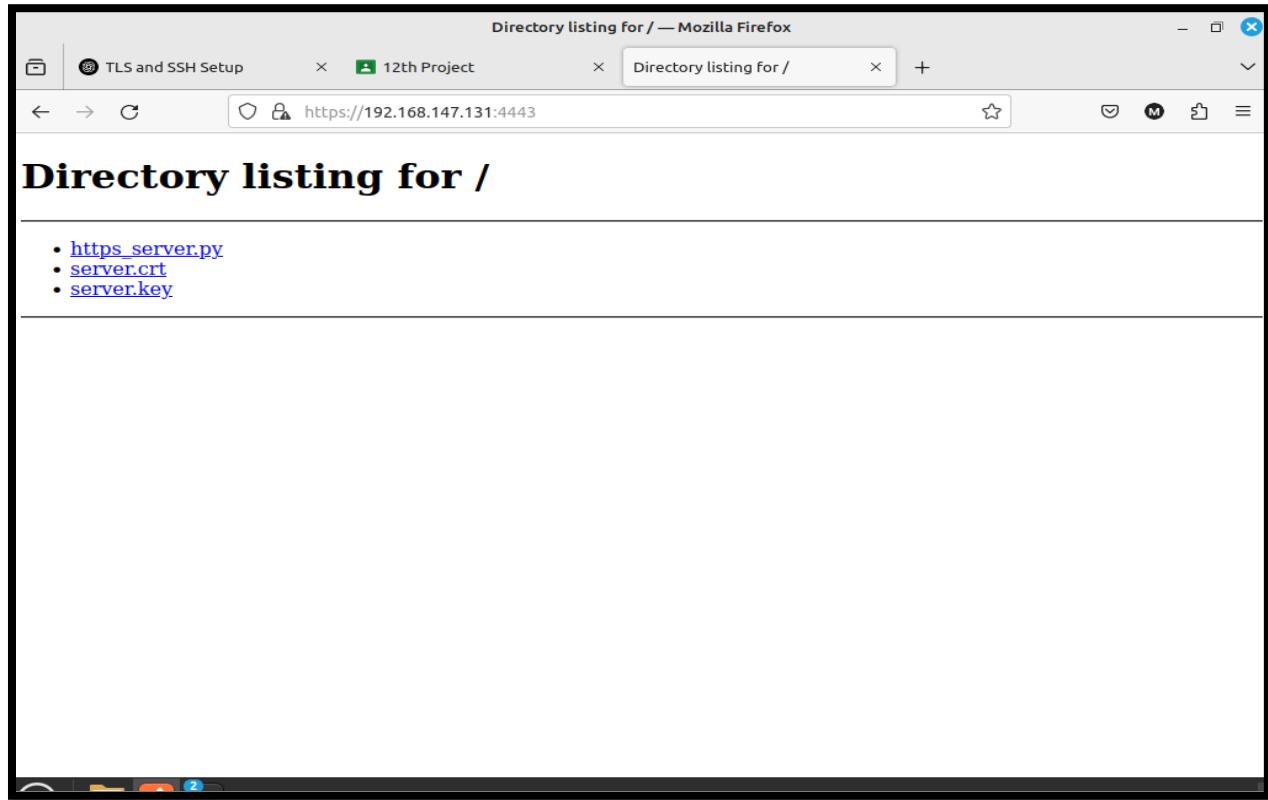


From the client (Linux Mint - Client)

Open terminal and test the connection using curl:

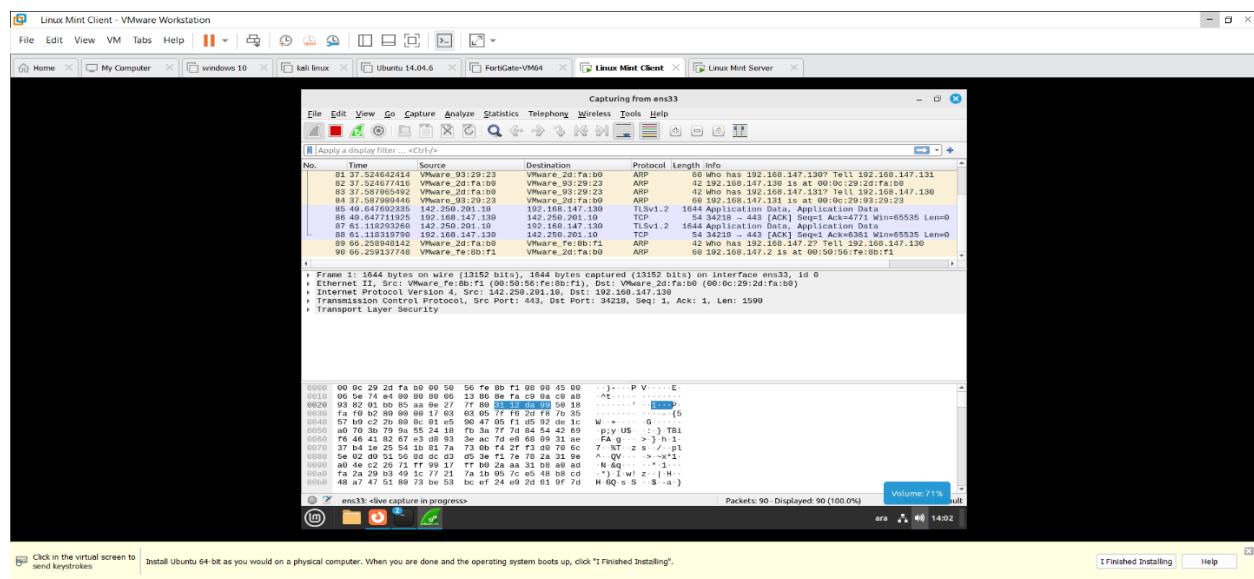


Or from browser:

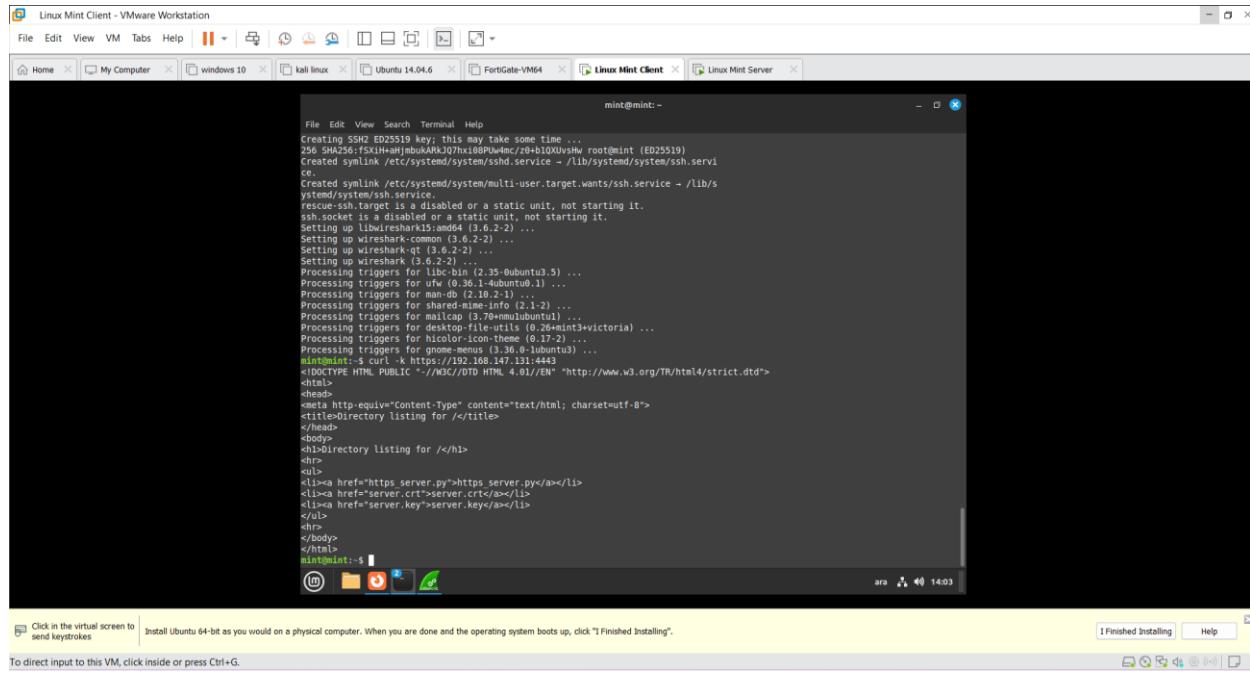


C) Capture & Decrypt TLS Traffic: Capture Encrypted TLS Traffic

Start Wireshark on the Serve

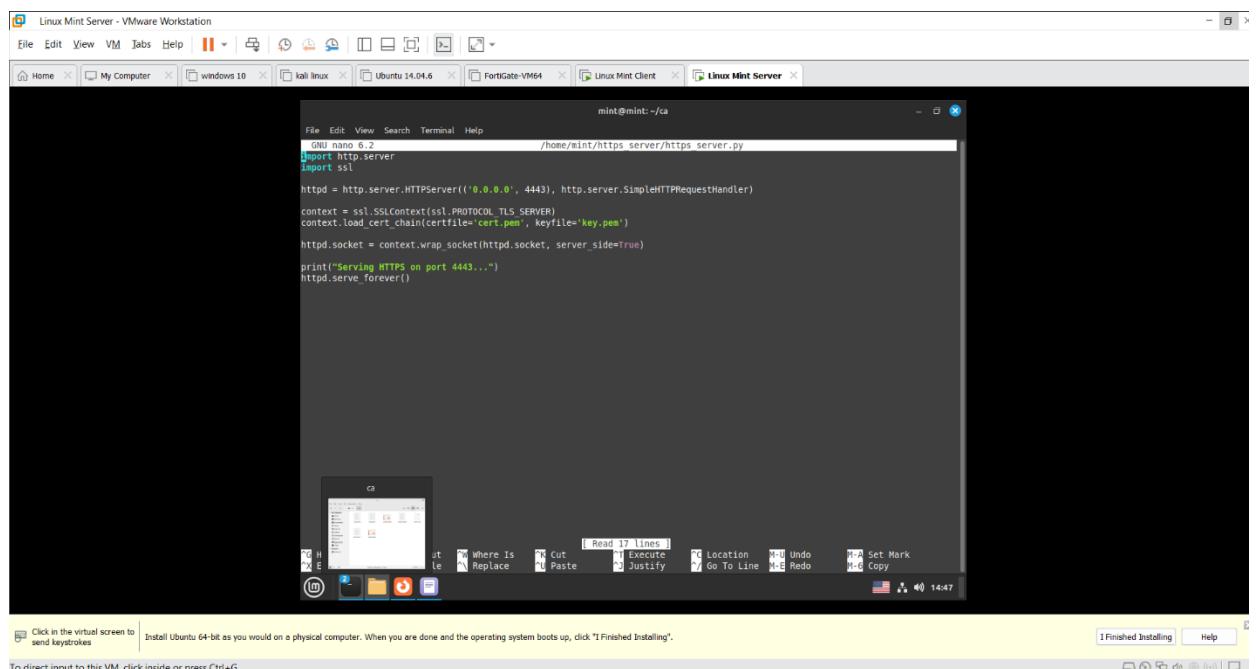
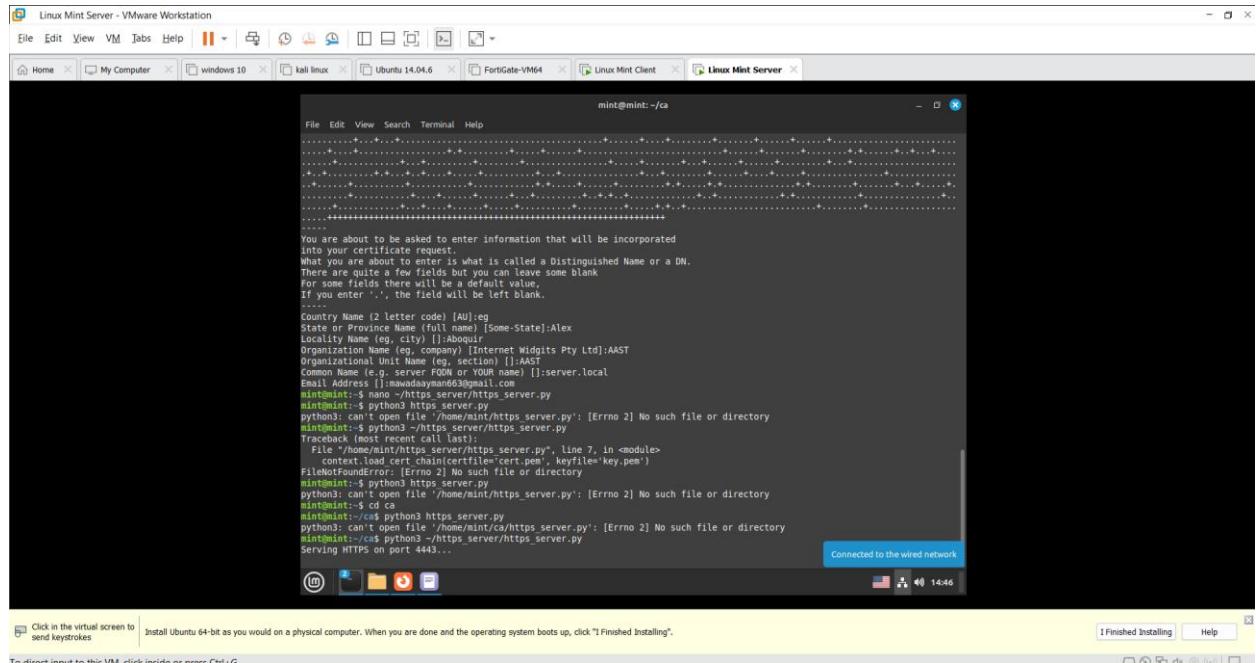


Connect from the Client



**Stop the Capture in Wireshark save as
tls_client_server_221003907/221003011.pcap**

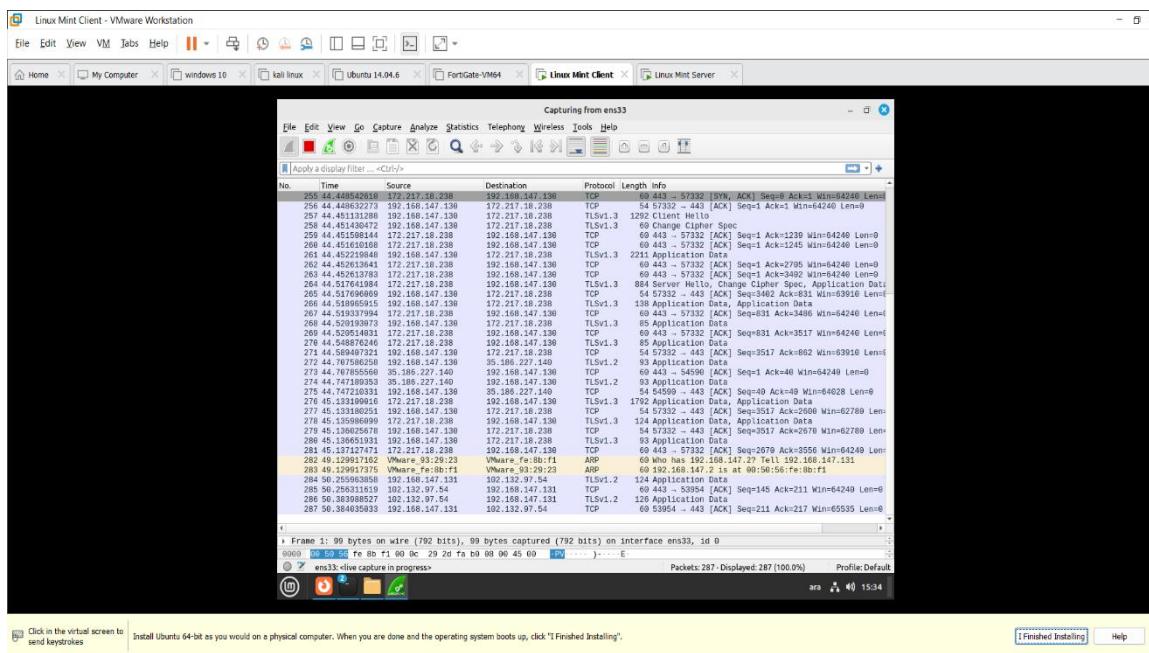
D)Decrypt TLS Traffic in Wireshark



Load the Session Key in Wireshark

On the Wireshark server machine:

1. Go to Edit → Preferences → Protocols → TLS (or SSL in some versions)
2. Set:
 - o (Pre)-Master-Secret log filename → Browse and select > /home/mint/https_server.keylog

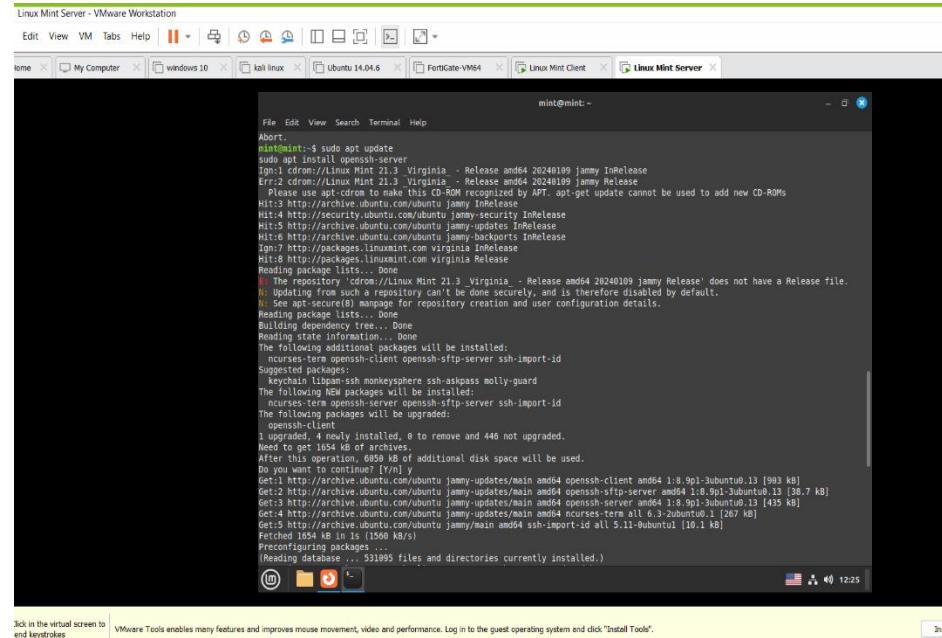


Part 2 (SSH):

SSH Configuration and Testing

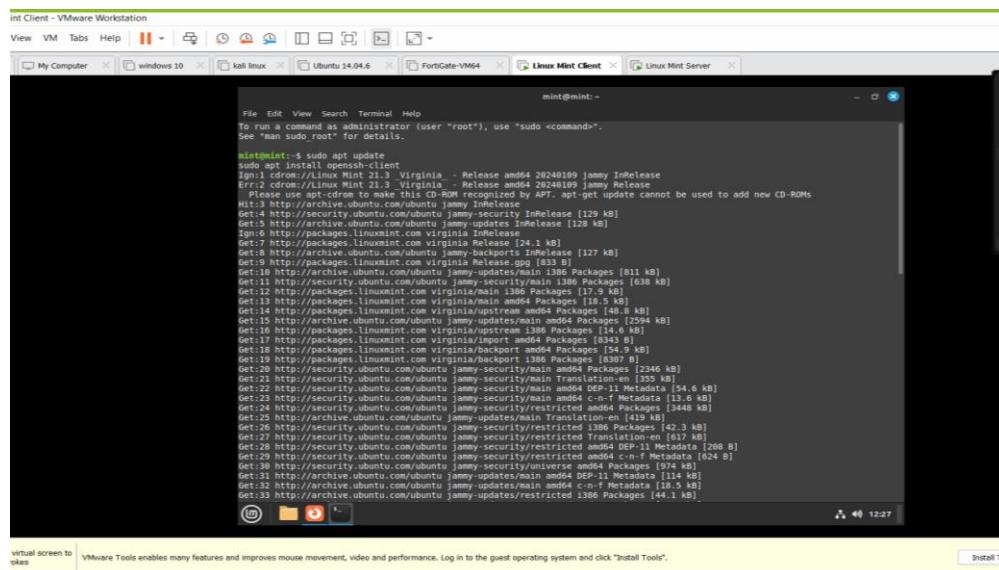
Step 1: Install SSH Server and Client

On the Server (Linux Mint Server):



```
mint@mint:~$ sudo apt update
sudo apt install openssh-server
Ign:2 cdrom:/Linux Mint 21.3 Virginia - Release amd64 20240109 jammy InRelease
Err:2 cdrom:/Linux Mint 21.3 Virginia - Release amd64 20240109 jammy InRelease
  Please use apt-cdrom to make this CD-ROM recognized by APT. apt-get update cannot be used to add new CD-ROMs
Hit:3 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:5 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:6 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Ign:7 http://packages.linuxmint.com virginia InRelease
Ign:8 http://packages.linuxmint.com virginia Release
Reading package lists...
W: Ignored: 'cdrom:/Linux Mint 21.3 Virginia - Release amd64 20240109 jammy Release' does not have a Release file.
W: Updating from such a repository can't be done securely, and is therefore disabled by default.
W: See apt-secure(8) manpage for repository creation and user configuration details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  transmission-gtk monit ssh-macsassas molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
J packages to upgrade, 0 newly installed, 0 to remove and 446 not upgraded.
Need to get 1654 kB of archives.
Do you want to continue? [yn]
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-client amd64 1:9.9p1-3ubuntu0.13 [903 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:9.9p1-3ubuntu0.13 [435 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 5.11-0ubuntu0.1 [267 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10.1 kB]
Fetched 1654 kB in 1s (1566 kB/s)
Preconfiguring packages...
(Reading database ... 531095 files and directories currently installed.)
(Reading database ... 531095 files and directories currently installed.)
```

On the Client (Linux Mint Client):

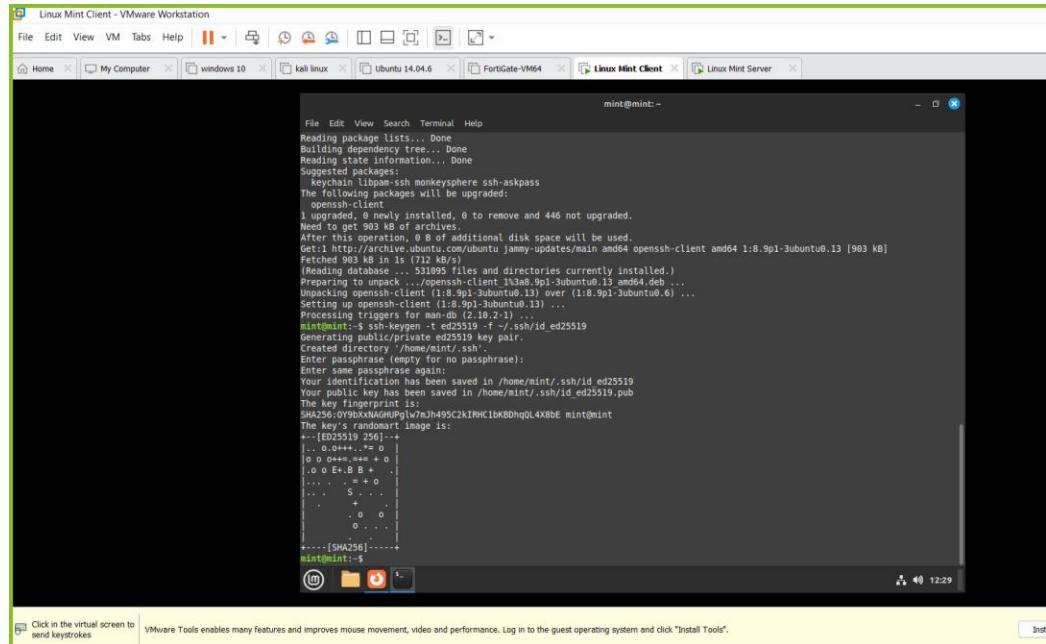


```
mint@mint:~$ sudo apt install openssh-client
Ign:1 http://archive.ubuntu.com/ubuntu jammy - Release amd64 20240109 jammy InRelease
Err:2 cdrom:/Linux Mint 21.3 Virginia - Release amd64 20240109 jammy InRelease
  Please use apt-cdrom to make this CD-ROM recognized by APT. apt-get update cannot be used to add new CD-ROMs
Hit:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Ign:5 http://packages.linuxmint.com/virginia/Release.gpg [24.1 kB]
Get:6 http://packages.linuxmint.com/virginia/Release [24.1 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1386 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [811 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [618 kB]
Get:11 http://packages.linuxmint.com/virginia/main 1386 Packages [17.9 kB]
Get:12 http://archive.ubuntu.com/ubuntu jammy/main amd64 Packages [13.6 kB]
Get:13 http://packages.linuxmint.com/virginia/main 1386 Packages [13.6 kB]
Get:14 http://packages.linuxmint.com/virginia/upstream amd64 Packages [40.8 kB]
Get:15 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [7294 kB]
Get:16 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1418 kB]
Get:17 http://packages.linuxmint.com/virginia/import amd64 Packages [6343 kB]
Get:18 http://packages.linuxmint.com/virginia/backport amd64 Packages [54.9 kB]
Get:19 http://archive.ubuntu.com/ubuntu jammy/main/binary-amd64/Packages [1346 kB]
Get:20 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1346 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [355 kB]
Get:22 http://archive.ubuntu.com/ubuntu jammy/main amd64 C-Header Metadata [13.6 kB]
Get:23 http://security.ubuntu.com/ubuntu jammy-security/main amd64 C-Header Metadata [13.6 kB]
Get:24 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [3448 kB]
Get:25 http://archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [419 kB]
Get:26 http://archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [1386 Packages] [42.3 kB]
Get:27 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [617 kB]
Get:28 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [208 B]
Get:29 http://archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [624 B]
Get:30 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [974 kB]
Get:31 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [114 kB]
Get:32 http://archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [617 kB]
Get:33 http://archive.ubuntu.com/ubuntu jammy-updates/restricted 1386 Packages [44.1 kB]
```

Step 2: Generate SSH Key Pairs

On the Client:

◊ Generate ED25519 key pair:



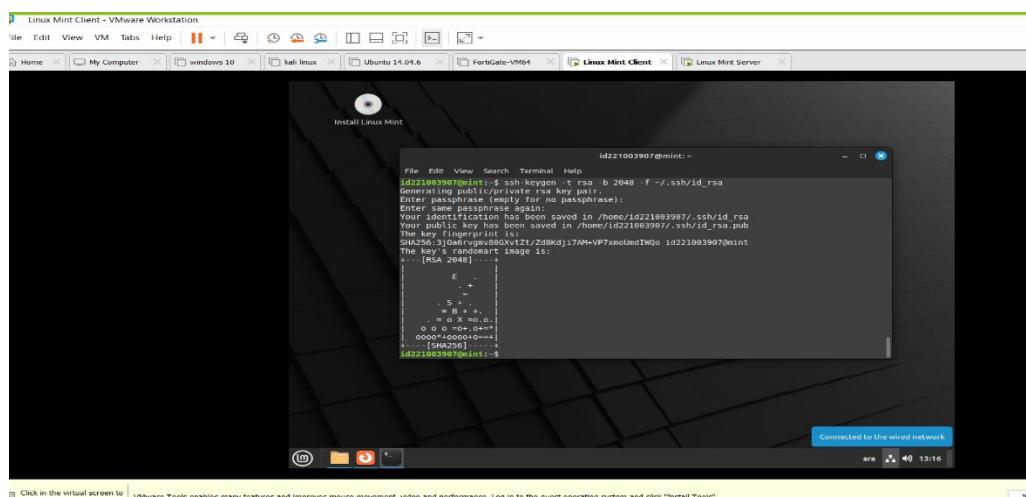
```
File Edit View Search Terminal Help
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  libkeychain libpam-ssh monkeysphere ssh-askpass
The following packages will be upgraded:
  openssh-client
1 upgraded, 0 newly installed, 0 to remove and 446 not upgraded.
Need to get 903 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-client amd64 1:8.9p1-3ubuntu0.13 [903 kB]
Fetched 903 kB in 1s (712 kB/s)
(Reading database ... 5390 files and directories currently installed.)
Preparing to unpack .../openssh-client_1:8.9p1-3ubuntu0.13_amd64.deb ...
Unpacking openssh-client (1:8.9p1-3ubuntu0.13) over (1:8.9p1-3ubuntu0.6) ...
Setting up openssh-client (1:8.9p1-3ubuntu0.13) ...
Processing triggers for man-db (2.17.1-0.5) ...
Generating public/private ed25519 key pair.
Created directory '/home/mint/.ssh'.
Enter passphrase (empty for no passphrase):
Enter passphrase again:
Your identification has been saved in /home/mint/.ssh/id_ed25519.
Your public key has been saved in /home/mint/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:09YxxXNaQUNg|w7JH495C2KIMhC1bKB0hqQL4XBhE mint@mint
The file contains the following image:
-[ED25519 256]-[SHA256]-
[...]
mint@mint:~$
```

Click in the virtual screen to send keystrokes

VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".

Inst

Generate RSA key pair (2048 bits):

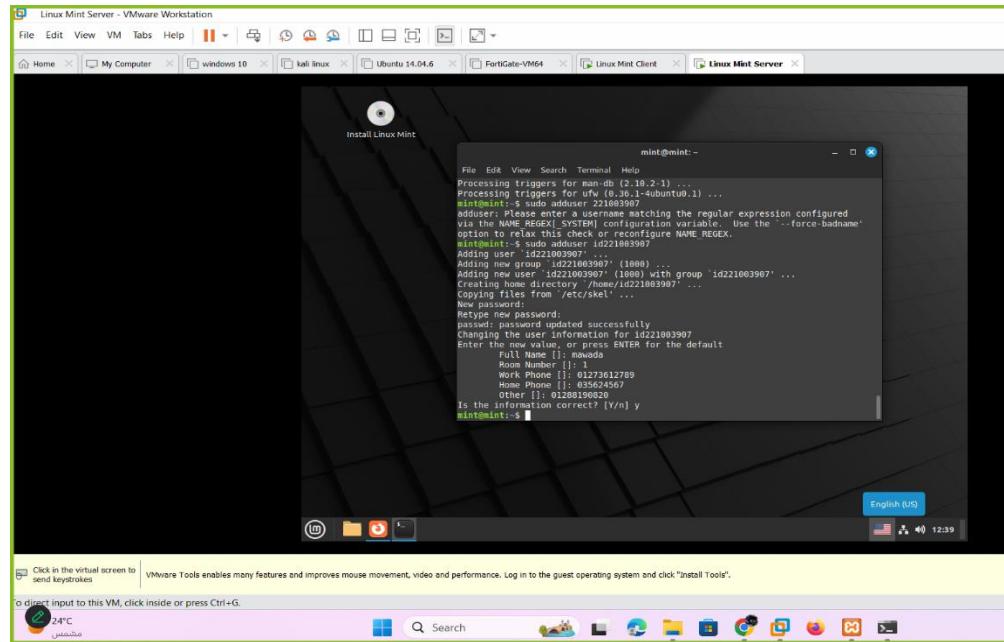


```
File Edit View Search Terminal Help
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter passphrase again:
Your identification has been saved in /home/id221003907/.ssh/id_rsa
Your public key has been saved in /home/id221003907/.ssh/id_rsa.pub
The file contains the following image:
-[RSA 2048]-[SHA256]-
[...]
id221003907@mint:~$
```

Connected to the wired network

Click in the virtual screen to

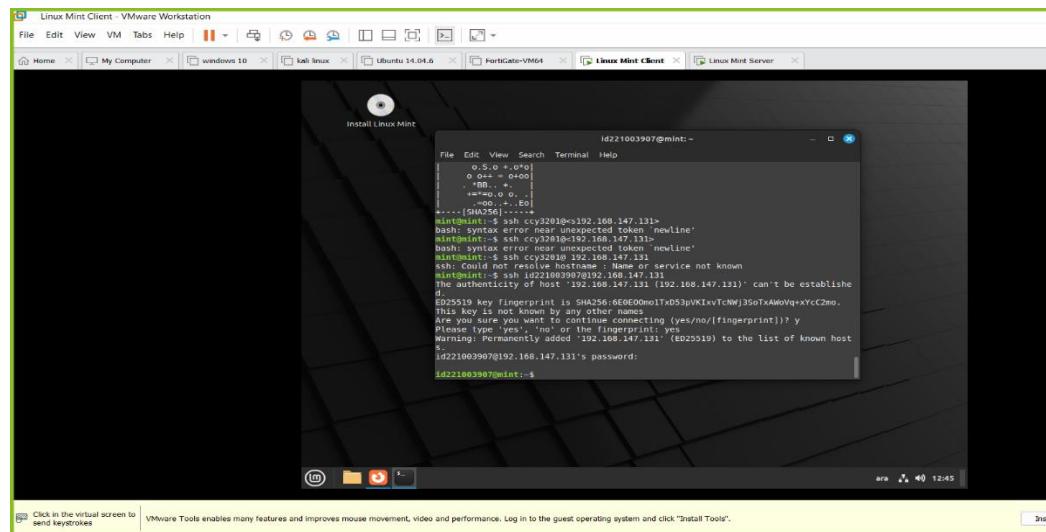
Step 3: Create a New User on the Server



Step 4: Test Password-Based SSH

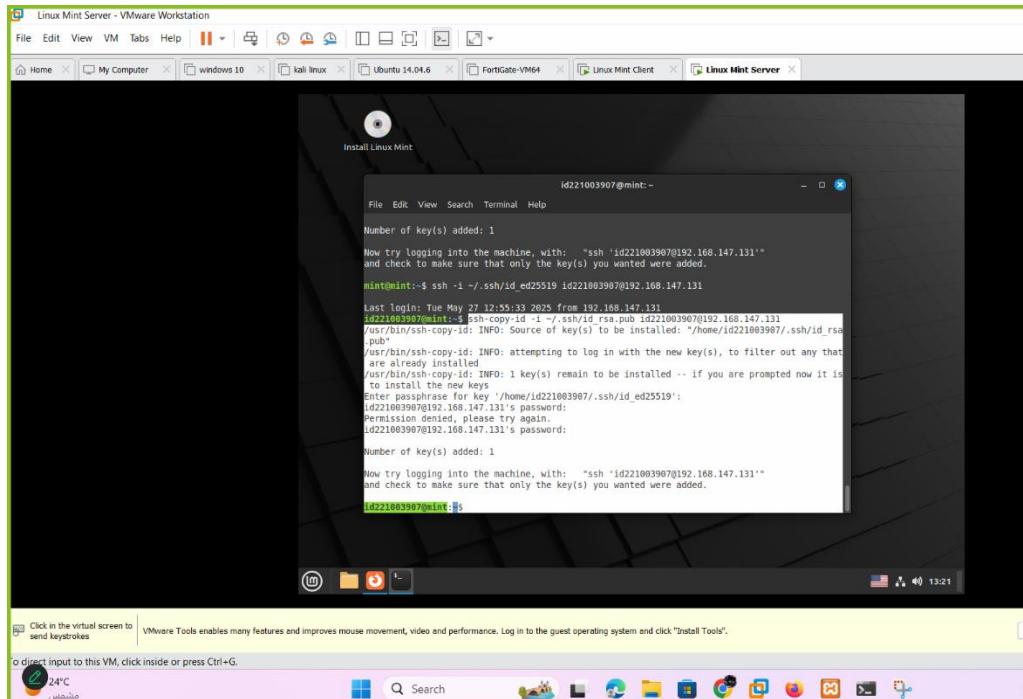
Login **Id221003907**

Password: mawada123

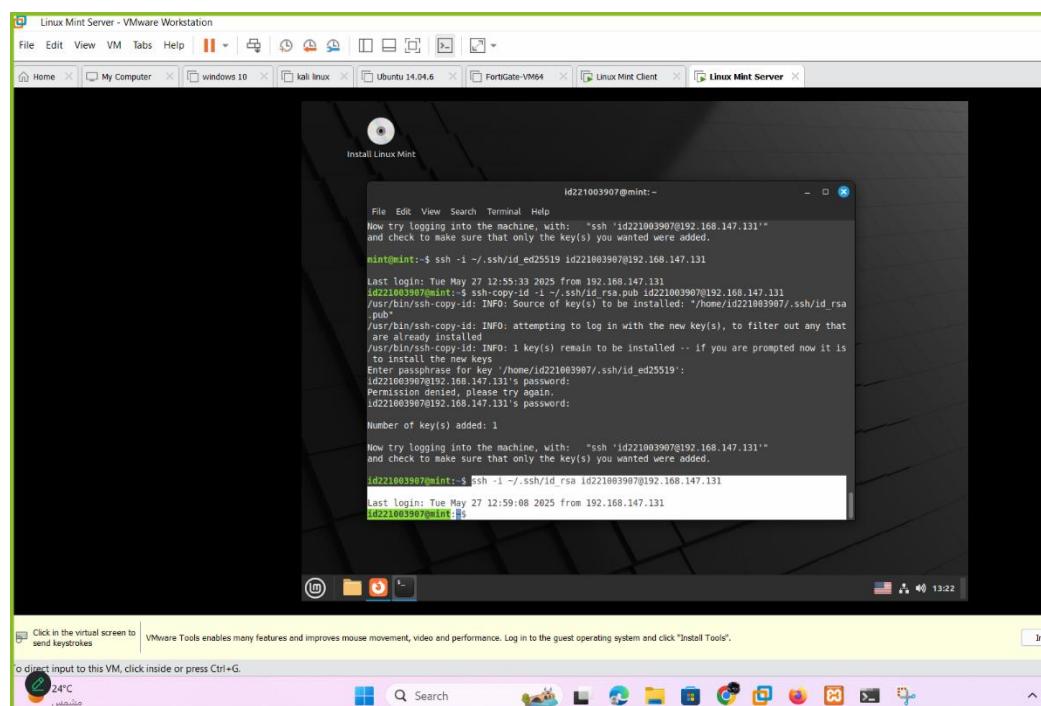


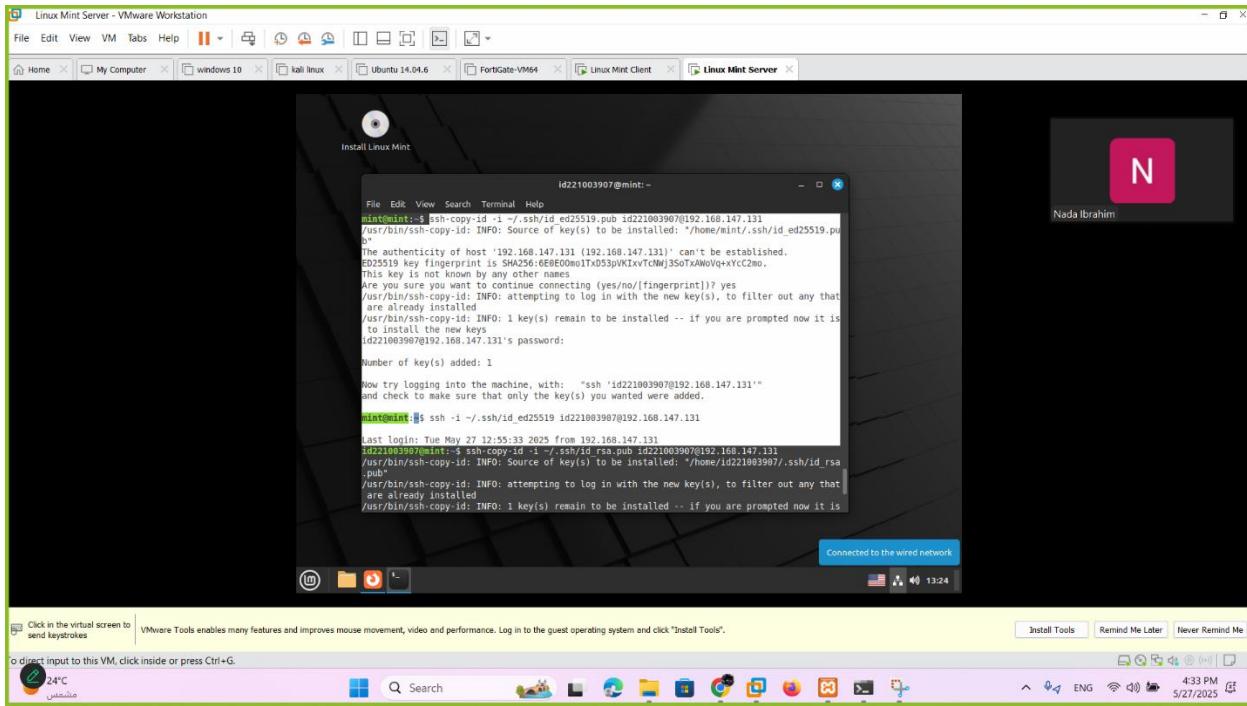
Step 5: Copy Public Key to the Server

Copy the ED25519 public key to the server:

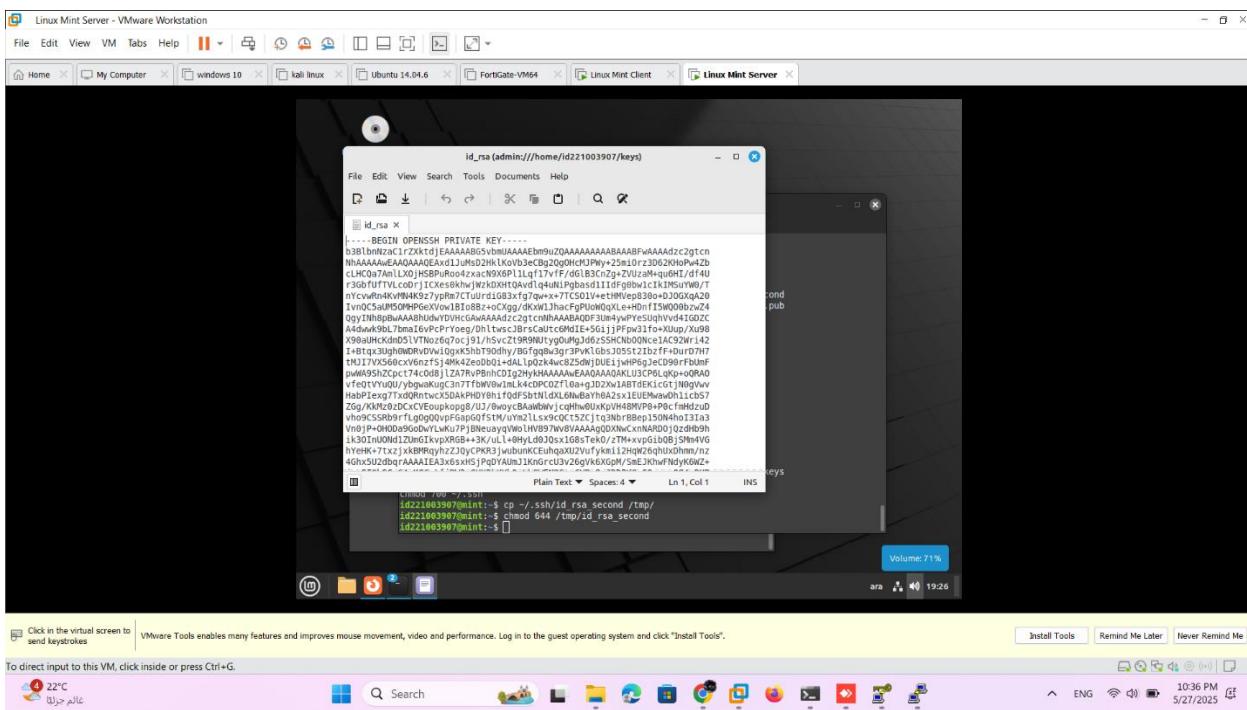


Then try to connect using the key:





Step 6: Generate key pairs on your client and copy the public key file to server through CLI, then connect using key-pairs.



Step 7 :Access Linux Server from Windows using PuTTY and RSA Key

1)Download PuTTY on windows (host)

2). Convert the Linux private key (id_rsa) to PuTTY format

1. Open PuTTYgen.

2. Click Load.

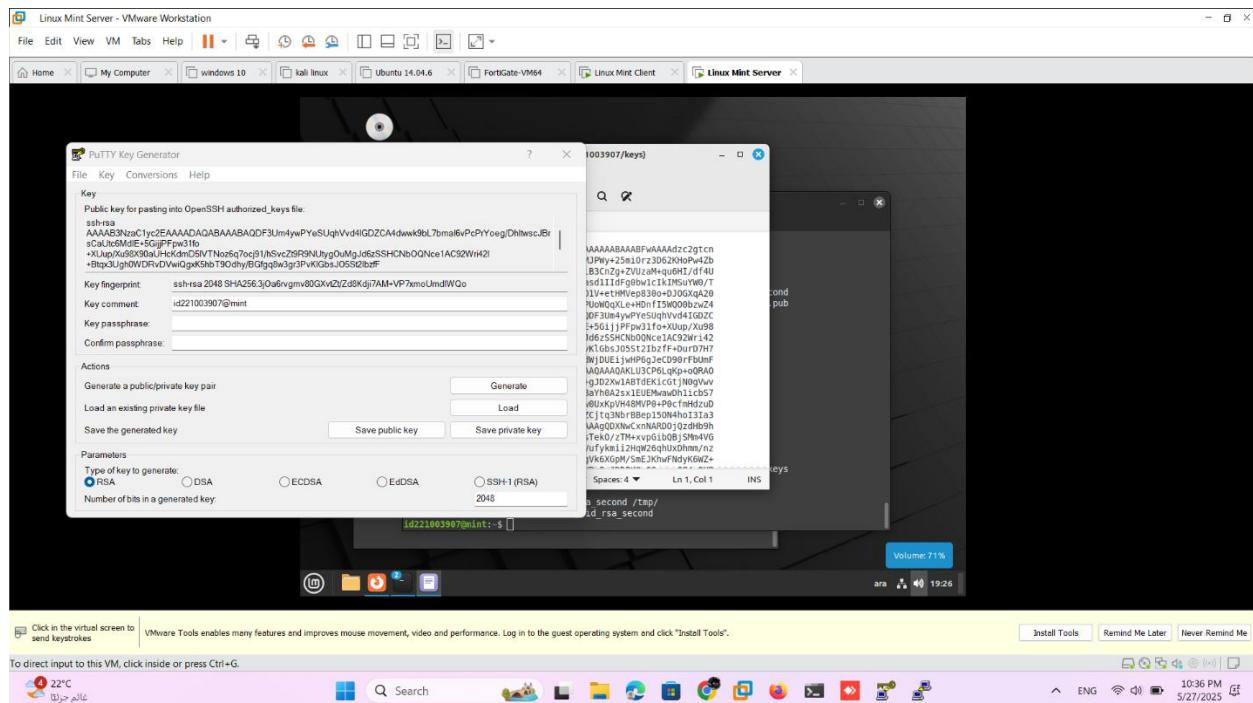
3. In the file dialog:

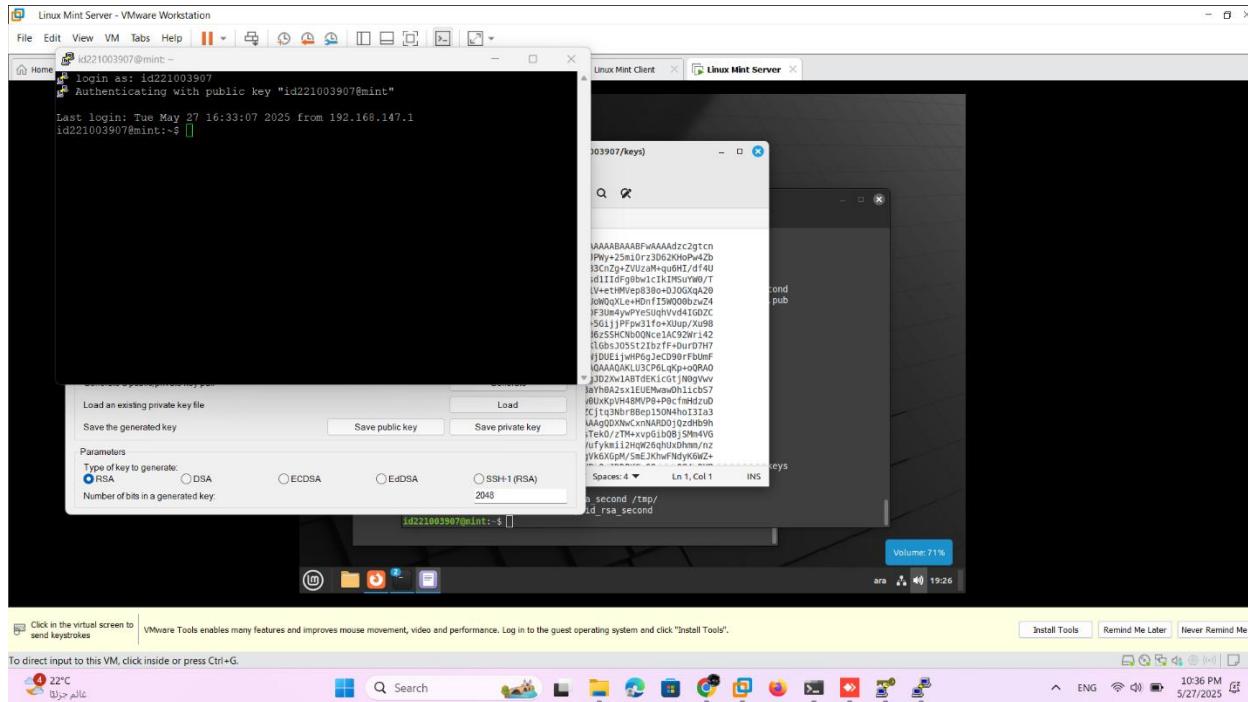
- Navigate to your id_rsa file from Linux (you need to copy it to Windows first using USB, WinSCP, or SCP).**
- Make sure you choose All Files (*) to see the id_rsa file.**

4. After it loads successfully, click Save private key.

- You can leave the passphrase empty or set one.**
- Save the file as something like id_rsa_windows.ppk.**

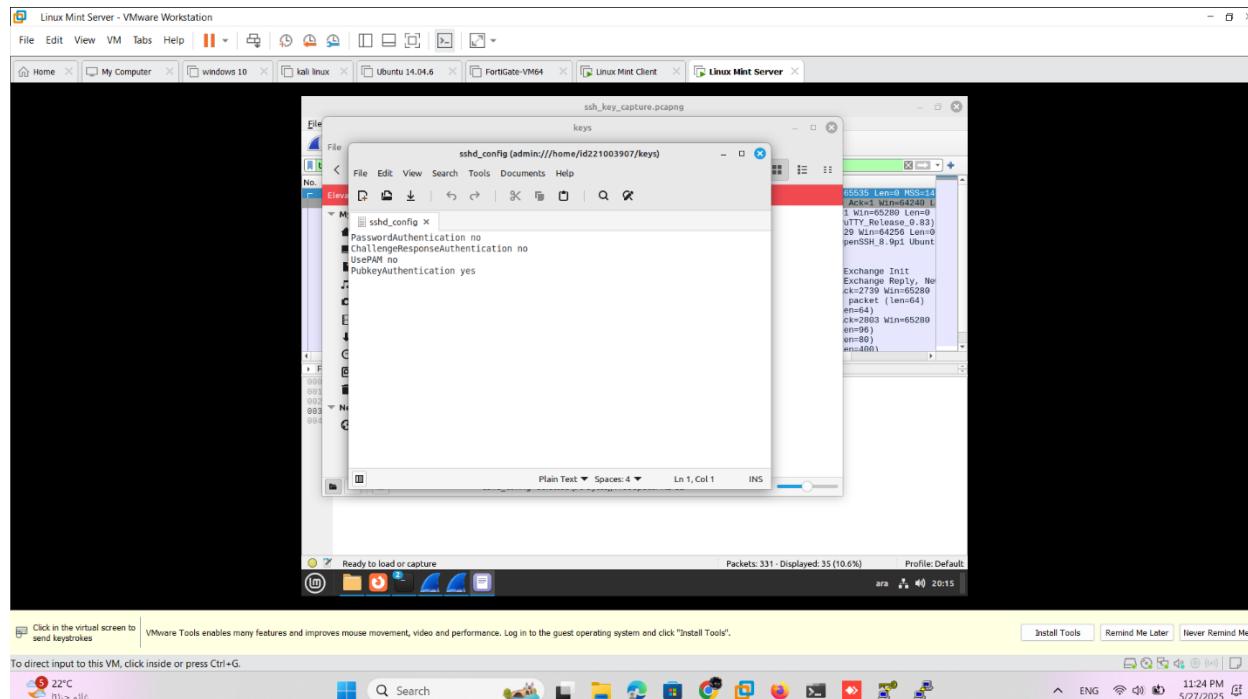
- **Use PuTTY to connect with the key:**
- **Open PuTTY.**
- **In the Host Name field:**
192.168.147.131
- **Port:22**
- **Go to:**
Connection > SSH > Auth
- **In the field: Private key file for authentication, browse and select your saved file:**
id_rsa_windows.ppk





Step 8: Disable Password Authentication and Enable Only Key-Based Login

Open the SSH configuration file on the server and modify the following lines:



- Capture traffic for SSH connection done using key-pairs

