الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

12thProject

Networks Security (CCY3201)

- **TA: Eng. Abdelrhman solyman**

Nada Ibrahim 221003011

Mawada Ayman 221003907

Lecturer: Dr. Ayman Adel

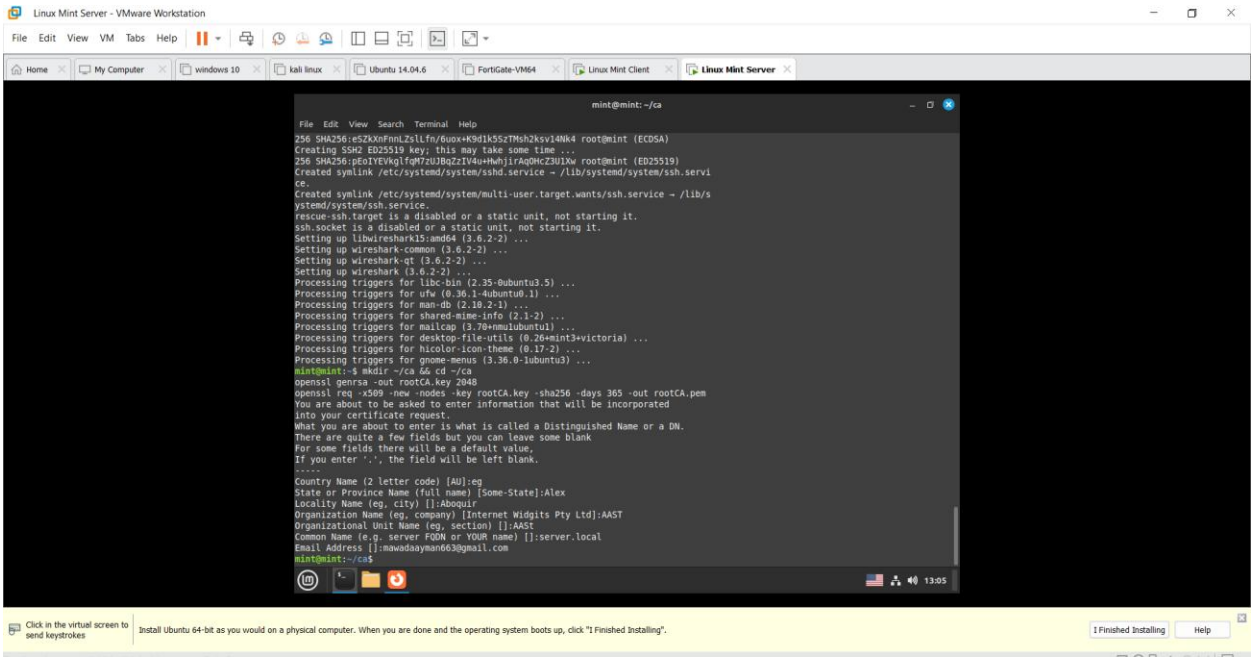
Course: Network Security

Part 1: TLS – HTTPS Web App Using OpenSSL

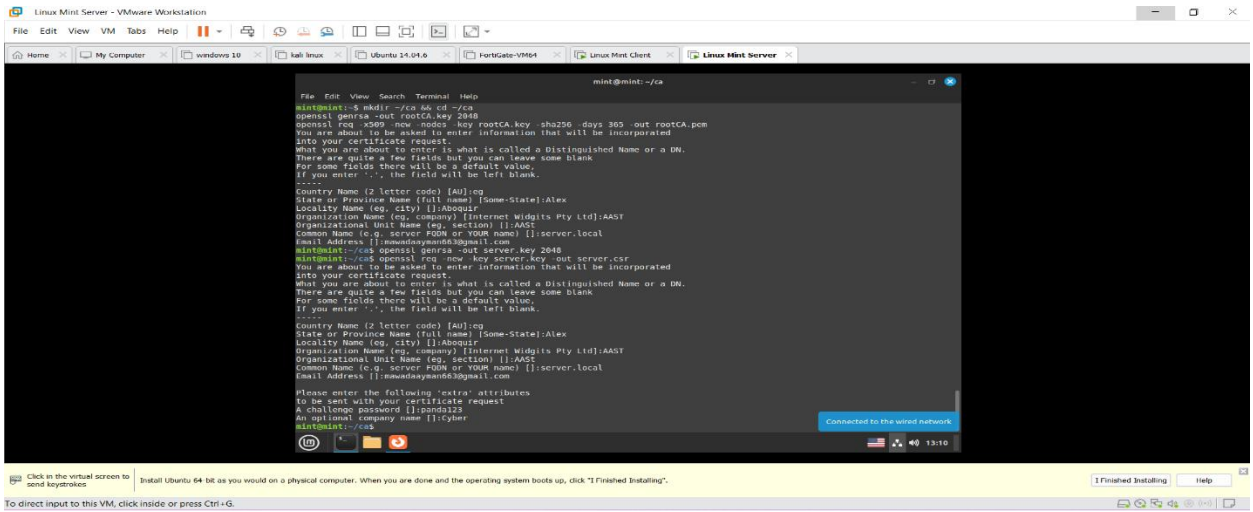
A) Generate Certificates Using OpenSSL

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

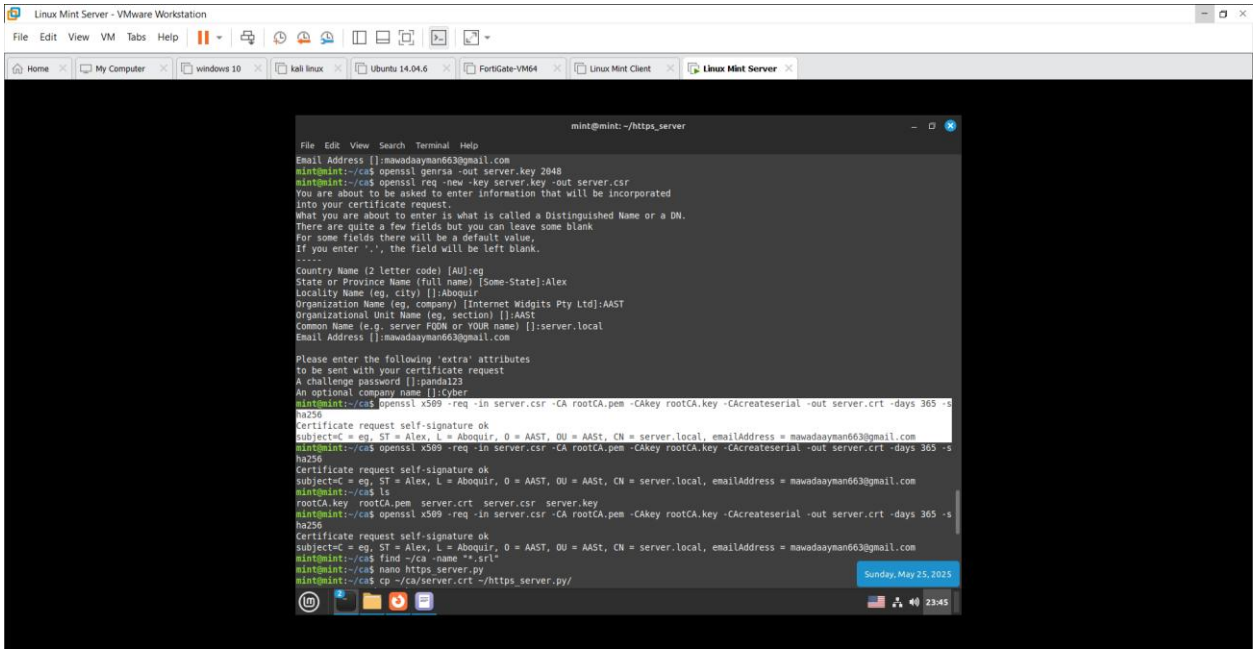
A. Create Root CA (on server VM)



B. Create Server Private Key and CSR

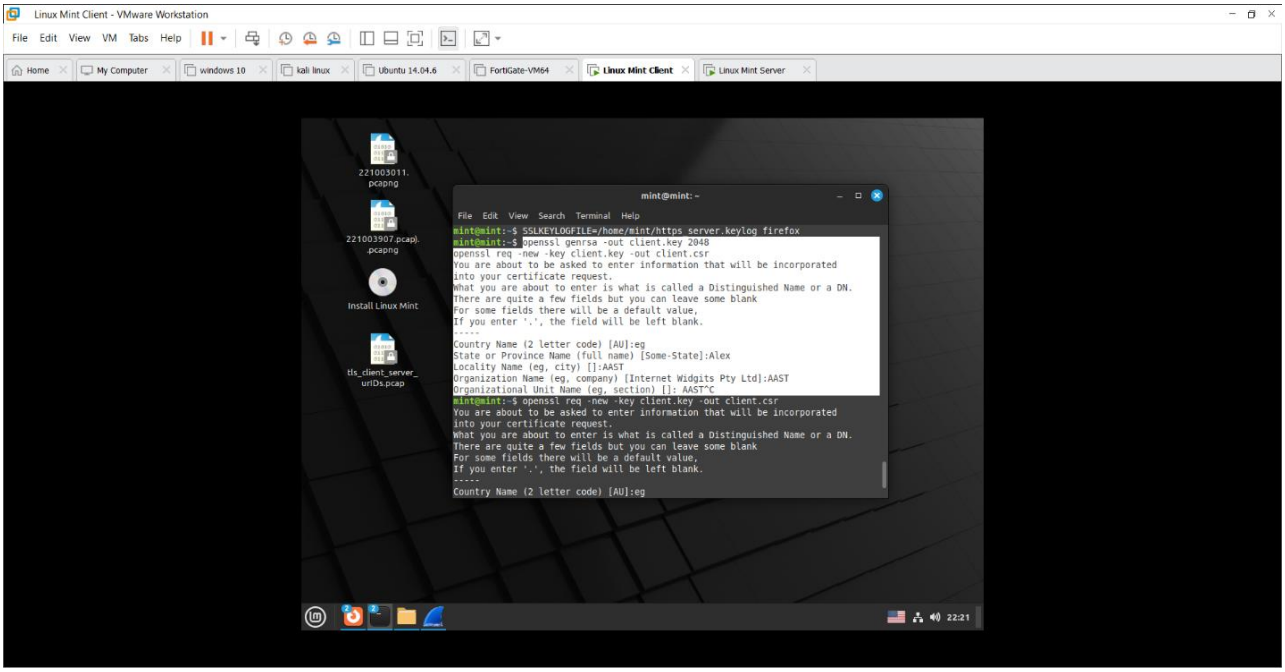


C. Sign Server Certificate with Root CA

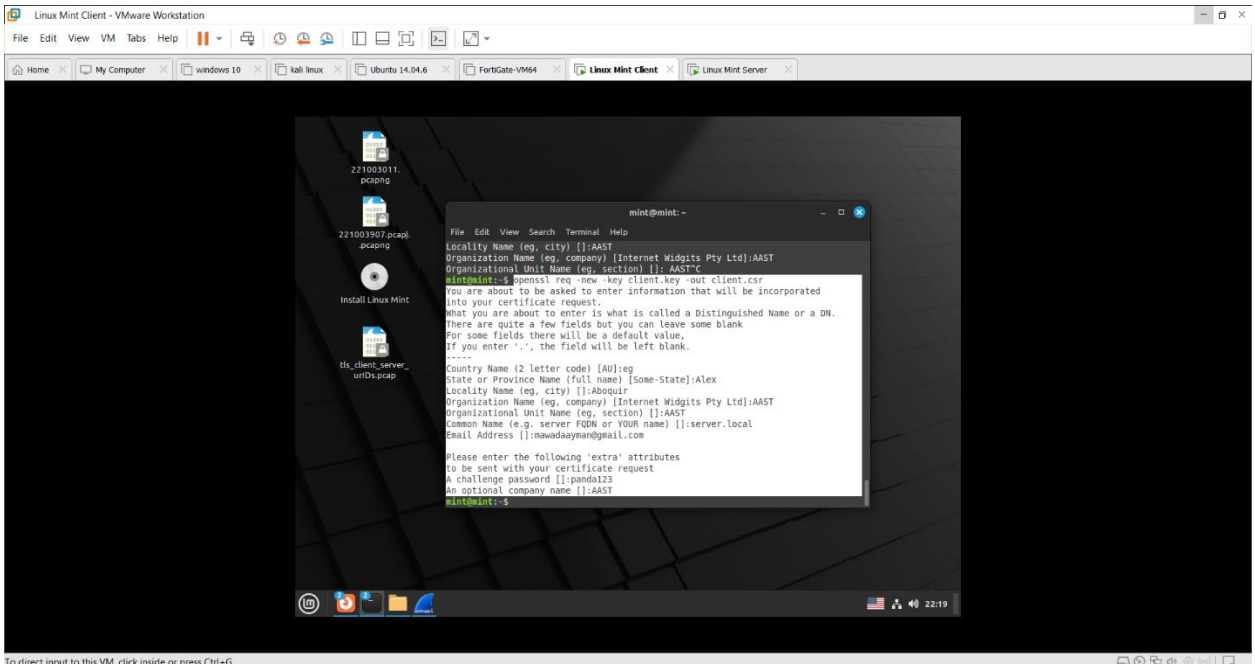


D. for Client Certificate

Generate client key and CSR



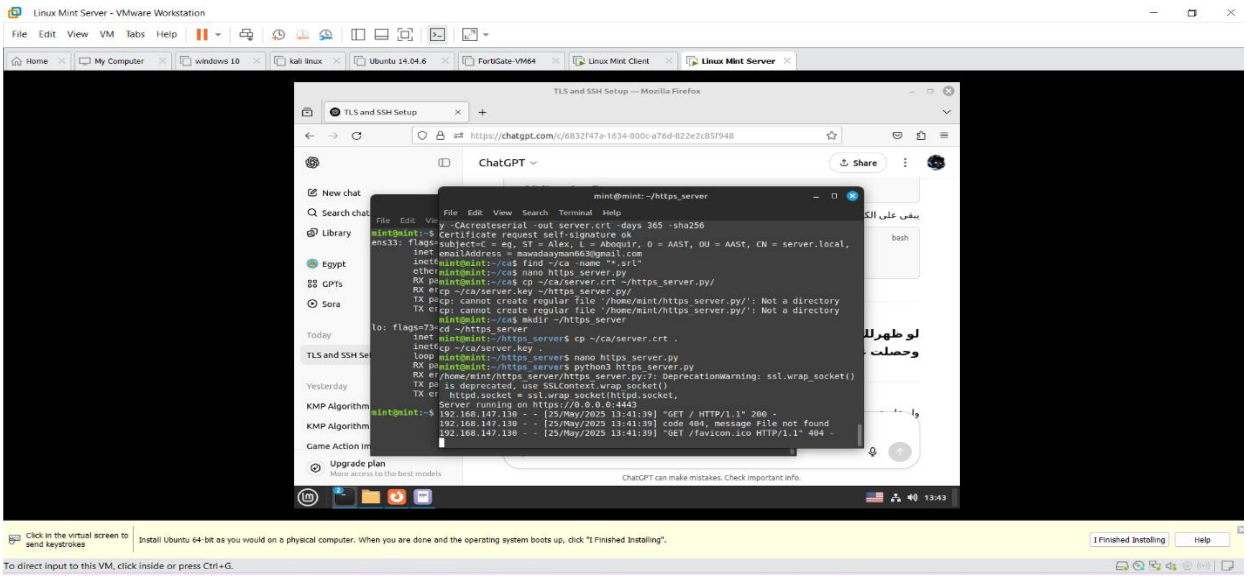
Sign client certificate with the same root CA

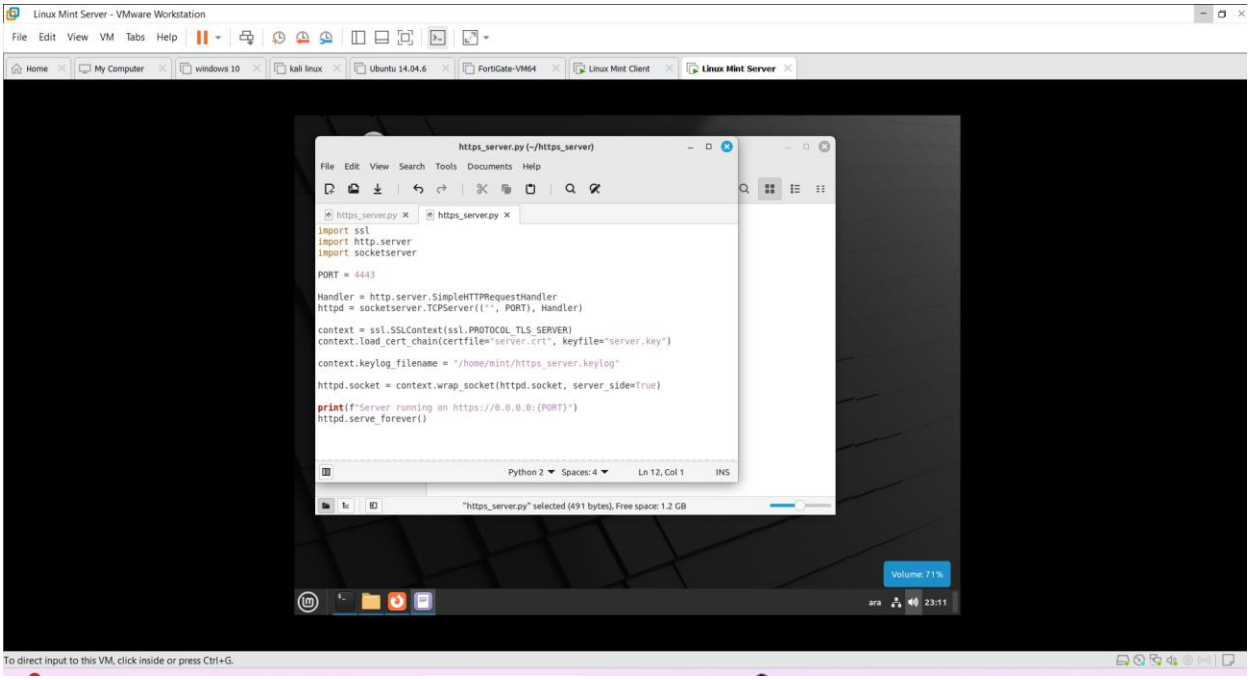


B)Simple TLS Client-Server App Server (Linux Mint Server)

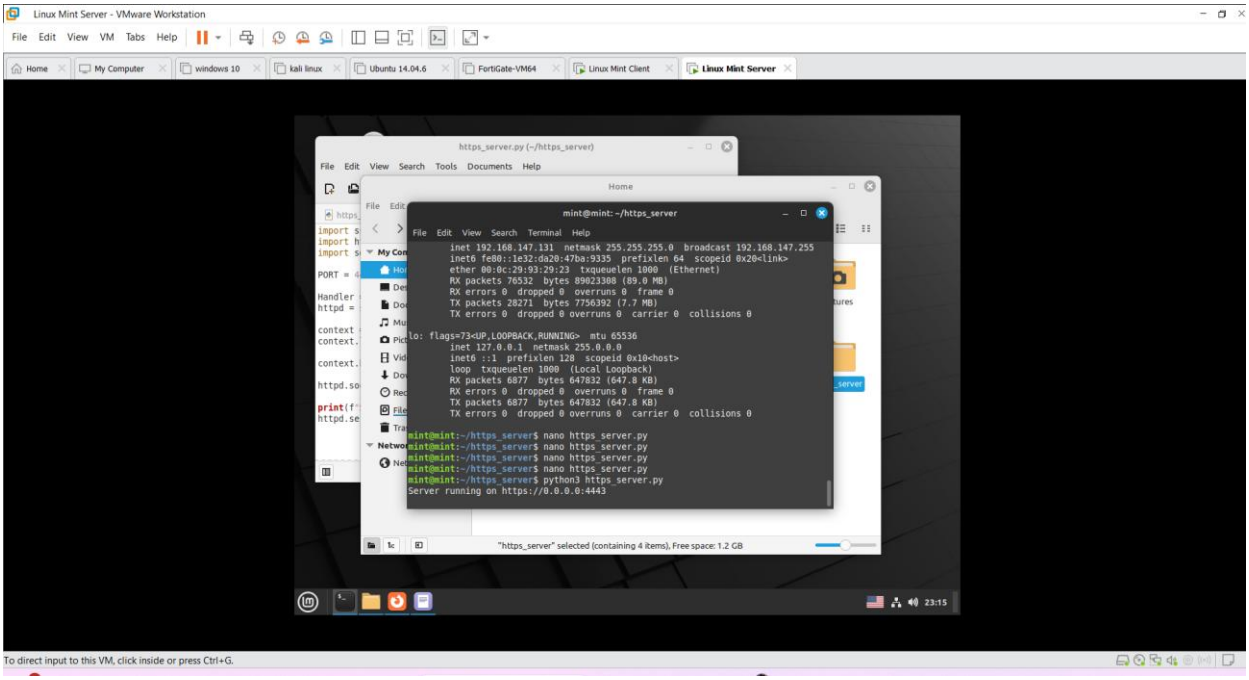
Step 1: Create the HTTPS server script

nano https_server.py



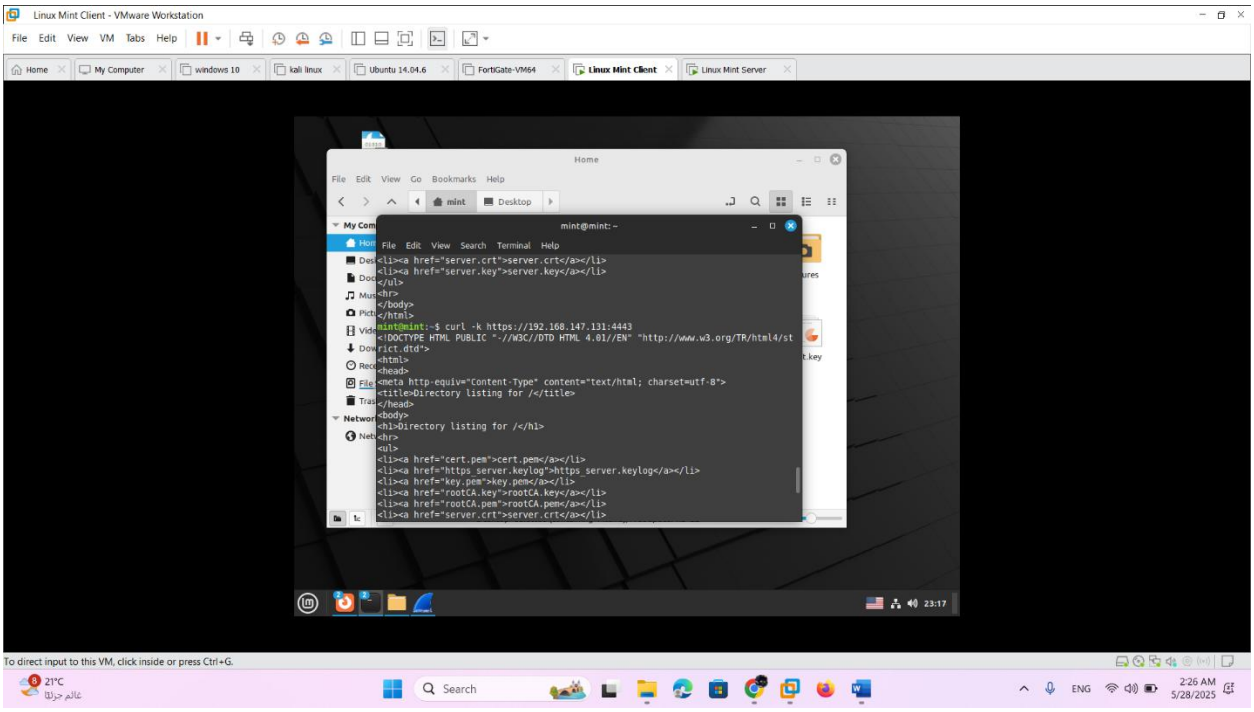


Step : Run the server

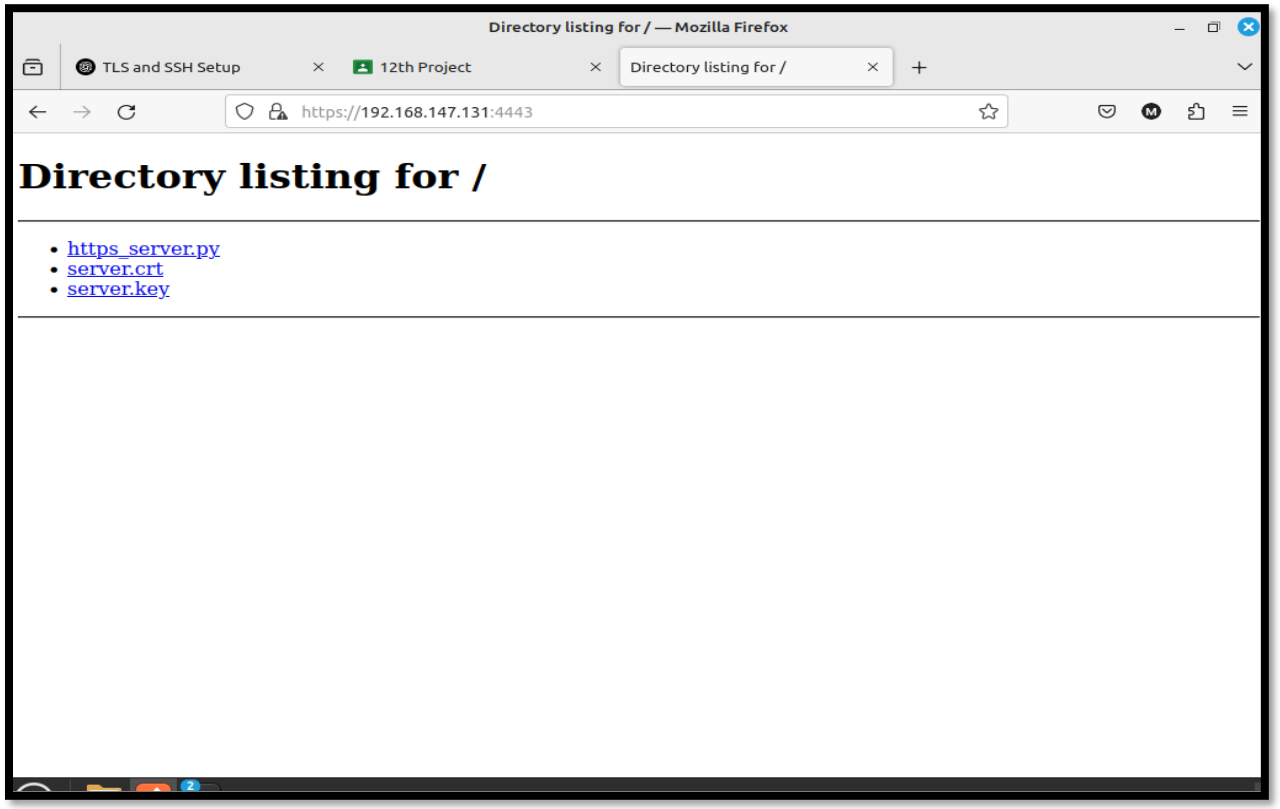


From the client (Linux Mint - Client)

Open terminal and test the connection using curl:

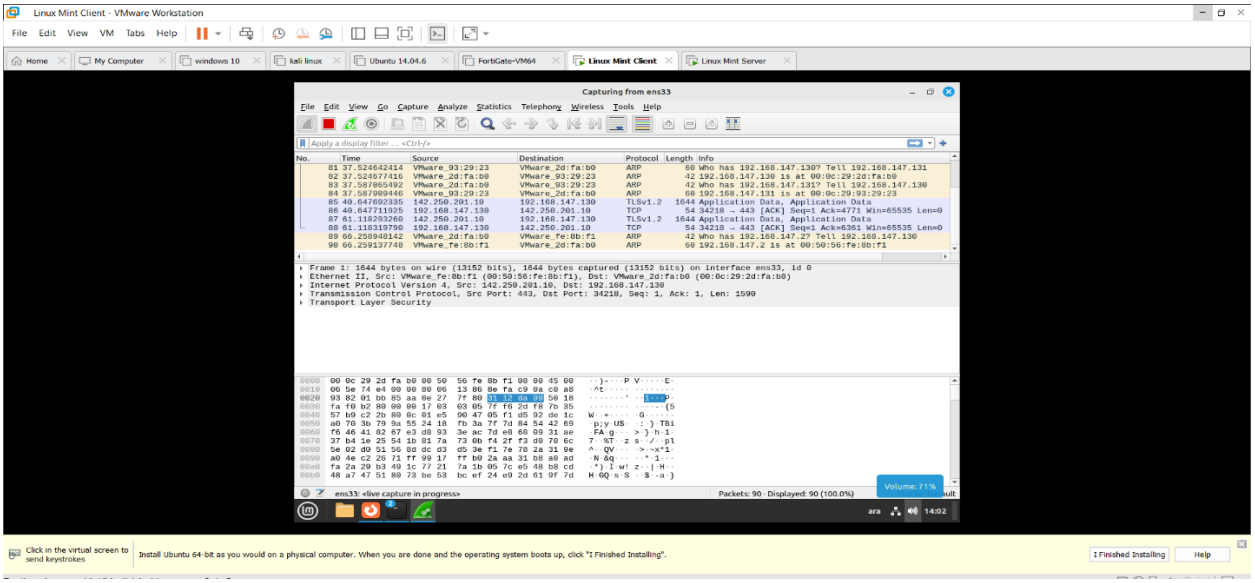


Or from browser:

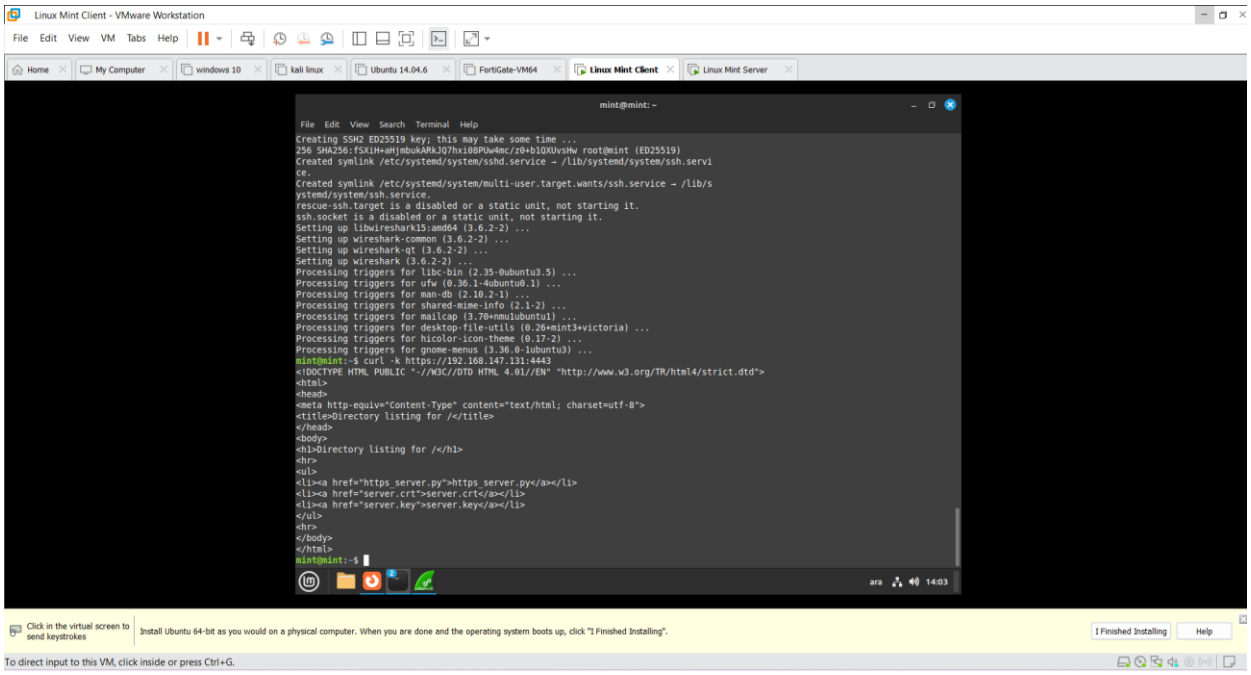


C) Capture & Decrypt TLS Traffic: Capture Encrypted TLS Traffic

Start Wireshark on the Serve

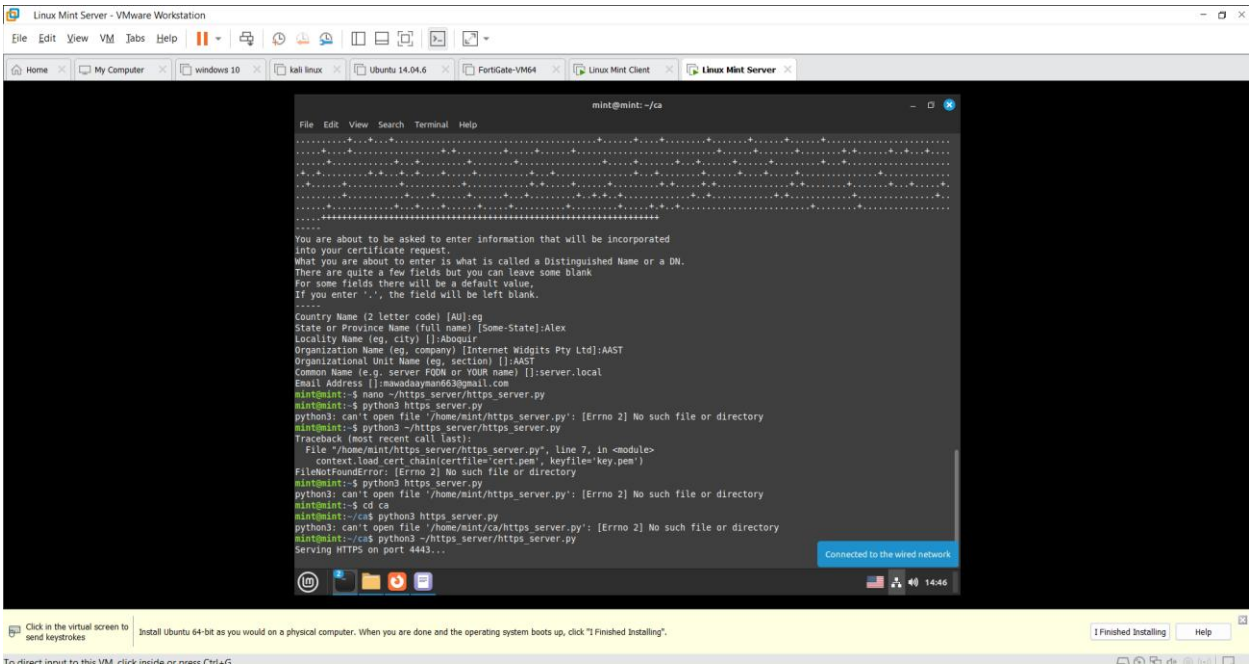


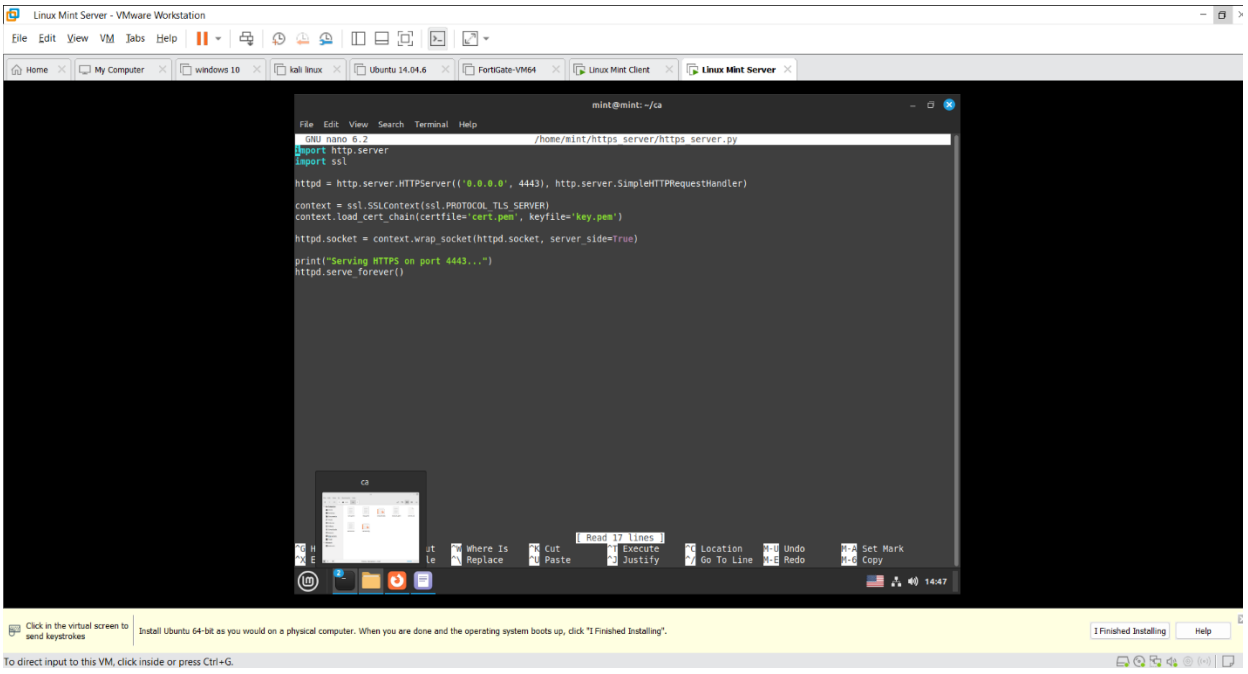
Connect from the Client



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

D) Decrypt TLS Traffic in Wireshark

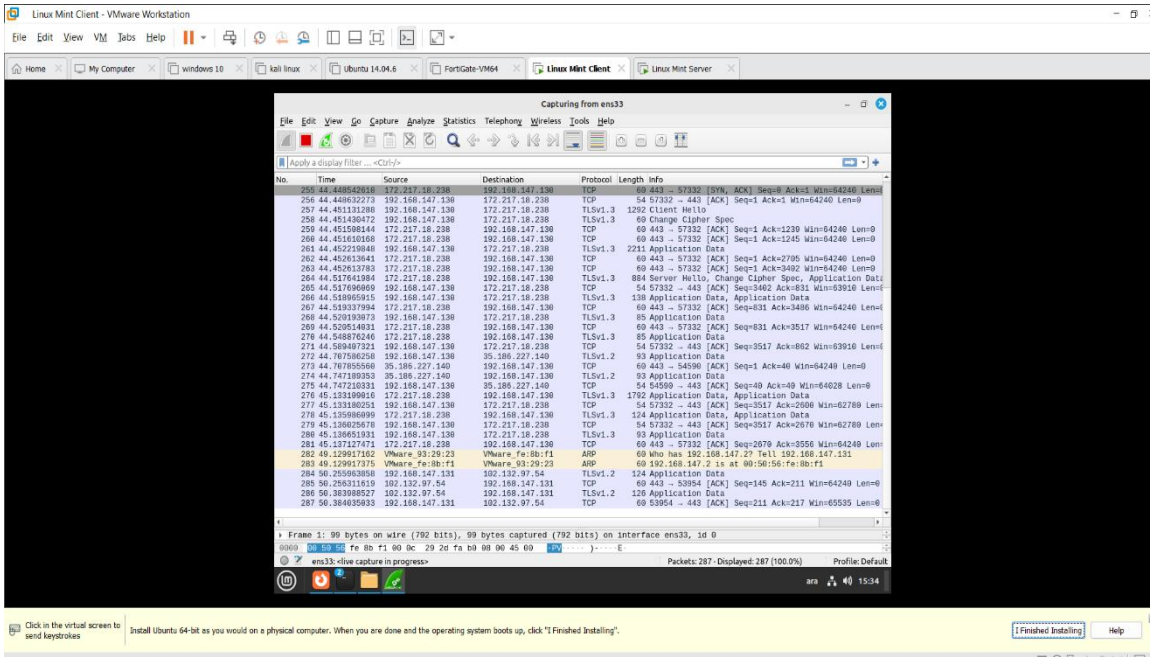




Load the Session Key in Wireshark

On the Wireshark server machine:

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

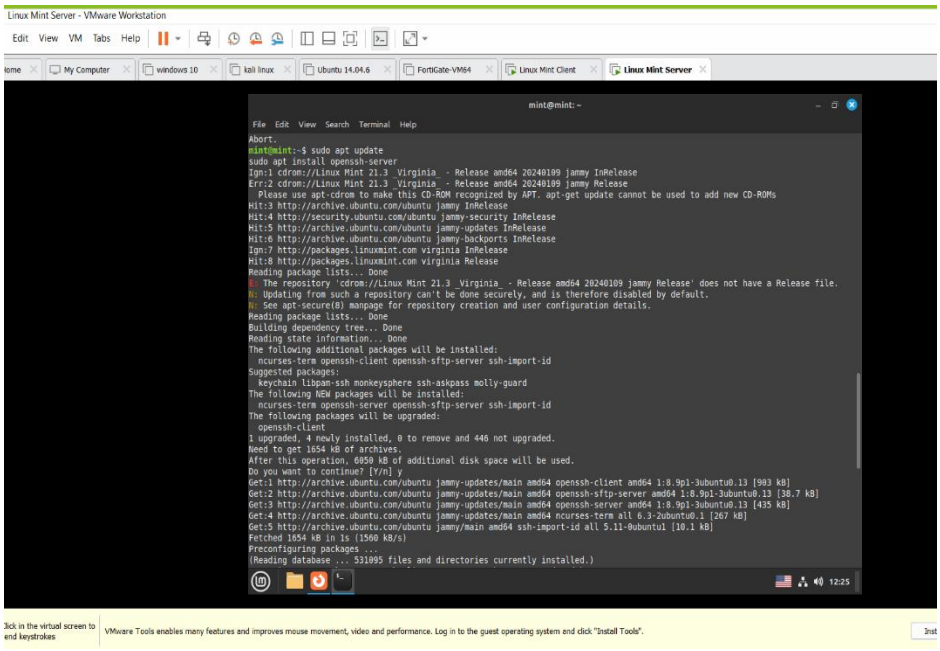


Part 2 (SSH):

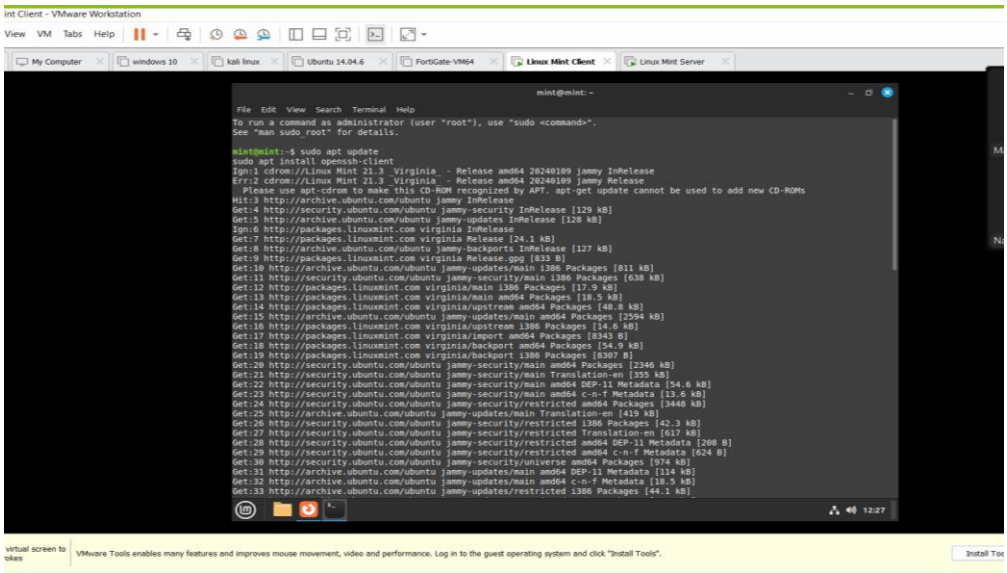
SSH Configuration and Testing

Step 1: Install SSH Server and Client

On the Server (Linux Mint Server):



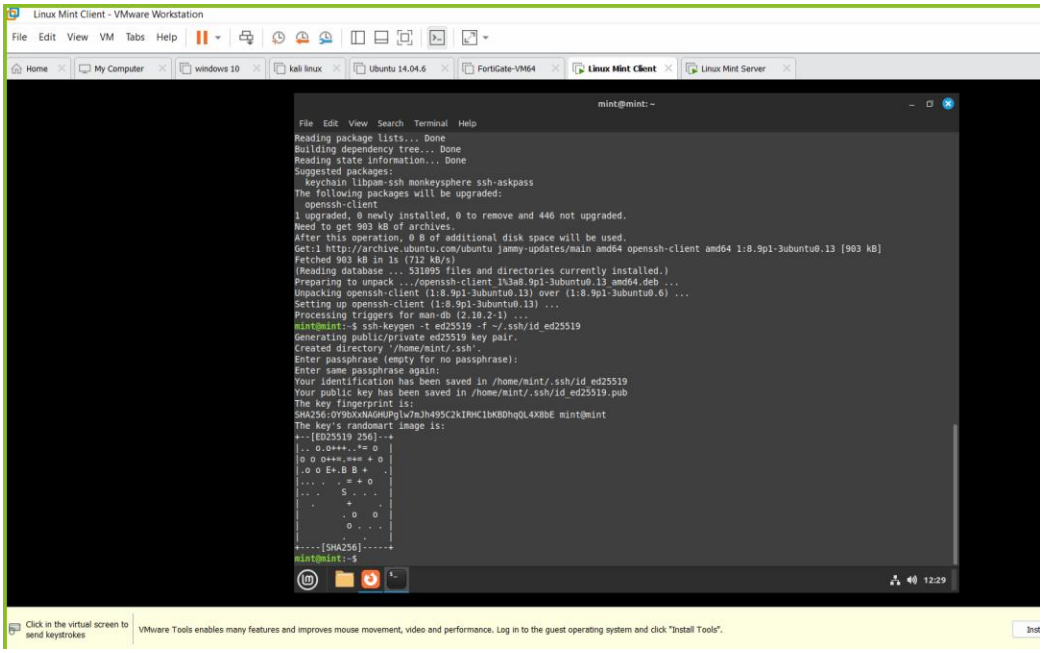
On the Client (Linux Mint Client):



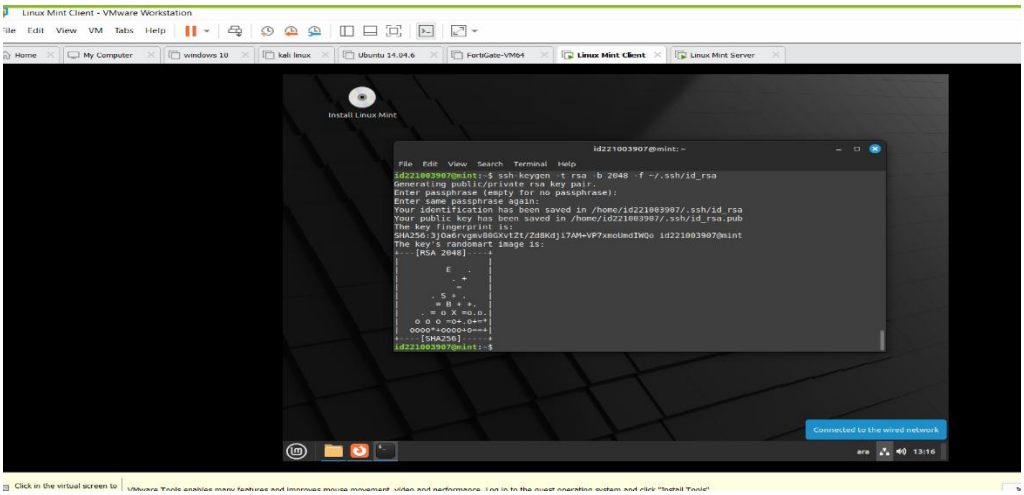
Step 2: Generate SSH Key Pairs

On the Client:

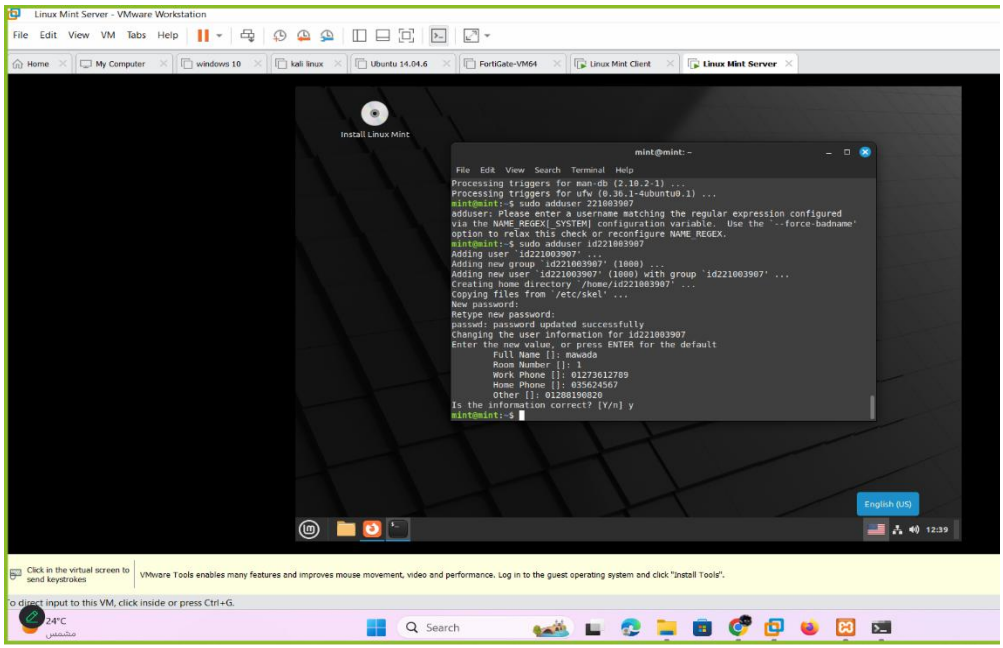
- ### Generate ED25519 key pair:



Generate RSA key pair (2048 bits):



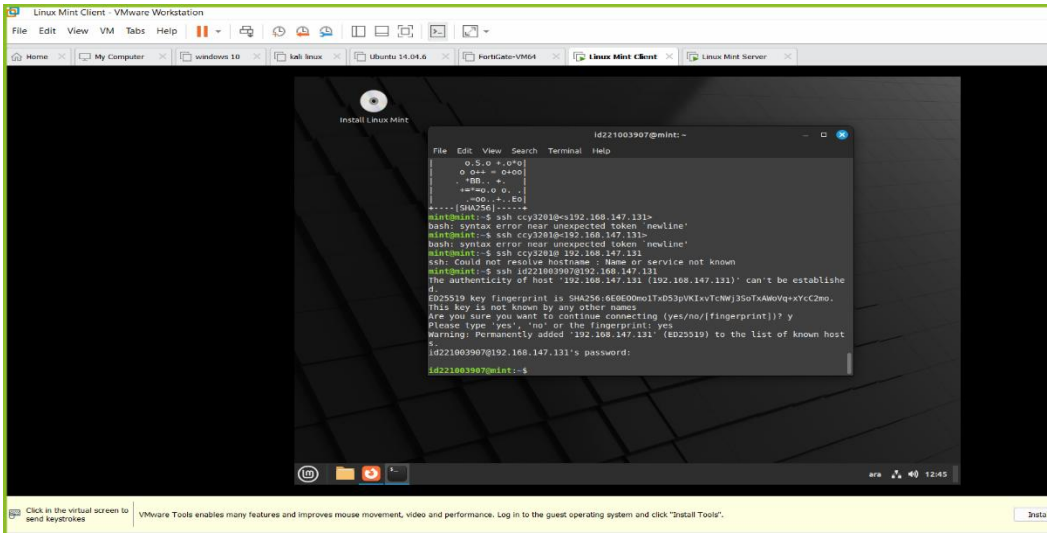
Step 3: Create a New User on the Server



Step 4: Test Password-Based SSH

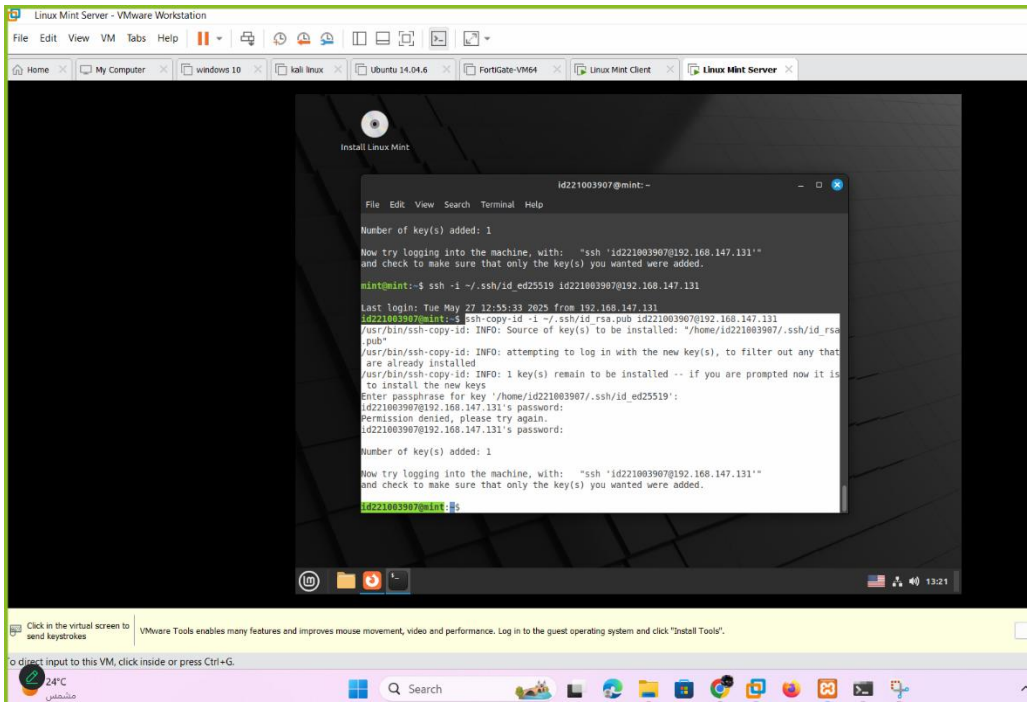
Login Id221003907

Password: mawada123

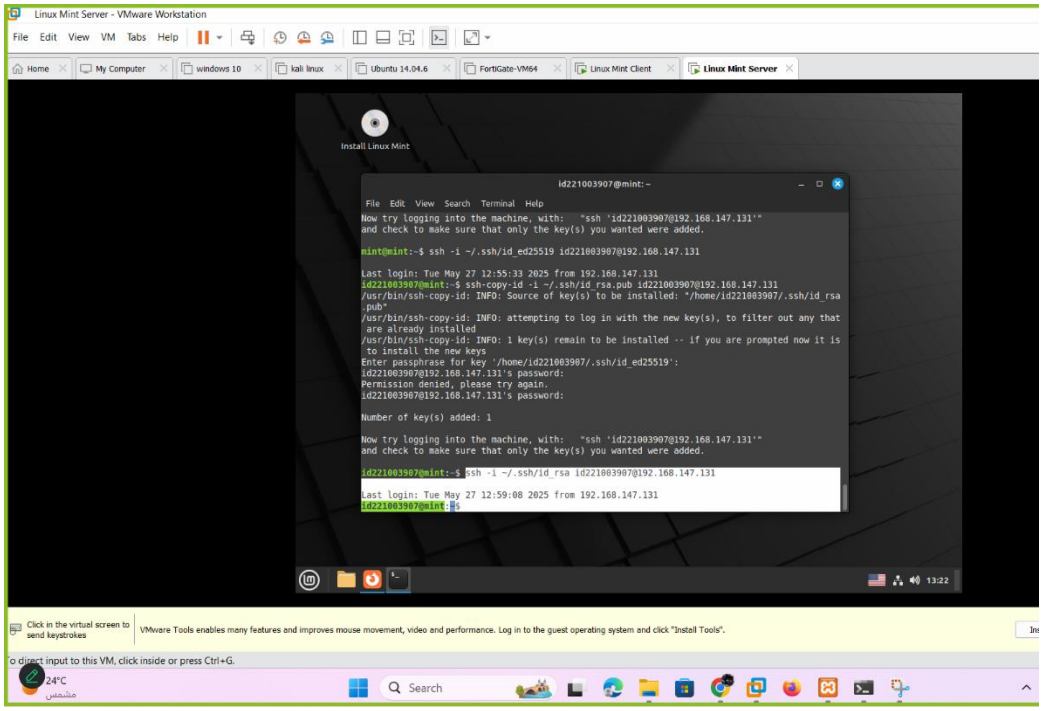


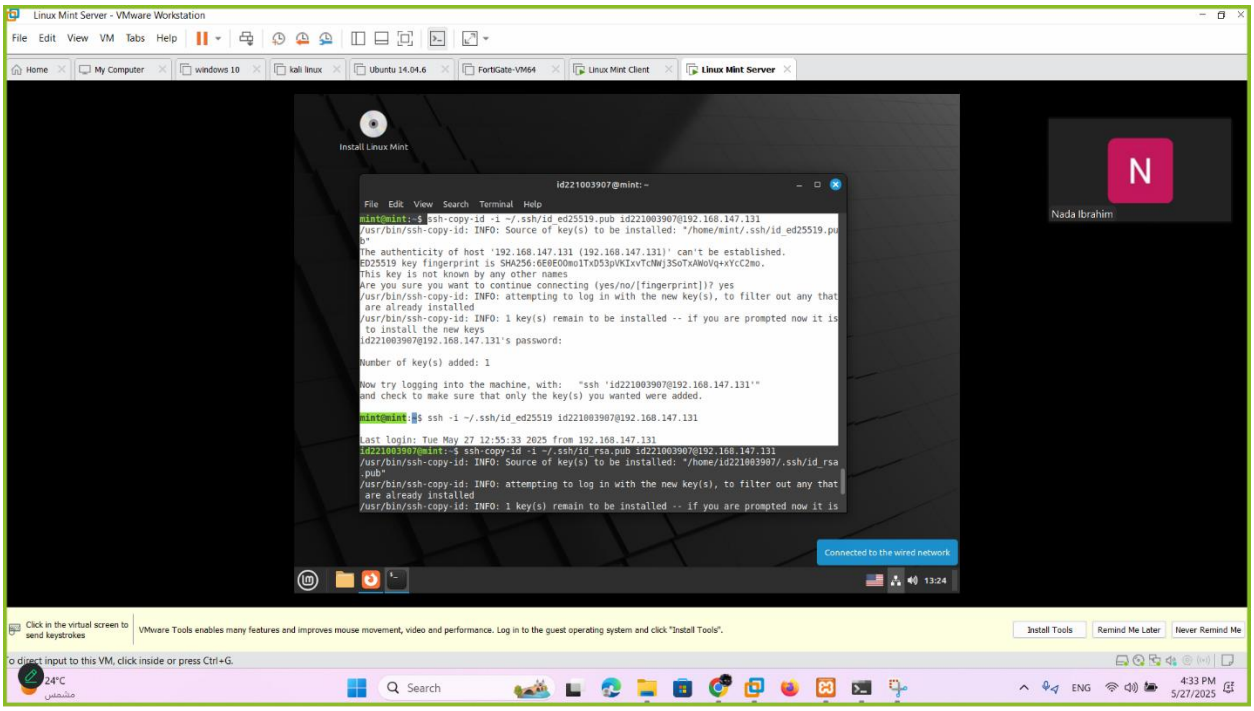
Step 5: Copy Public Key to the Server

Copy the ED25519 public key to the server:



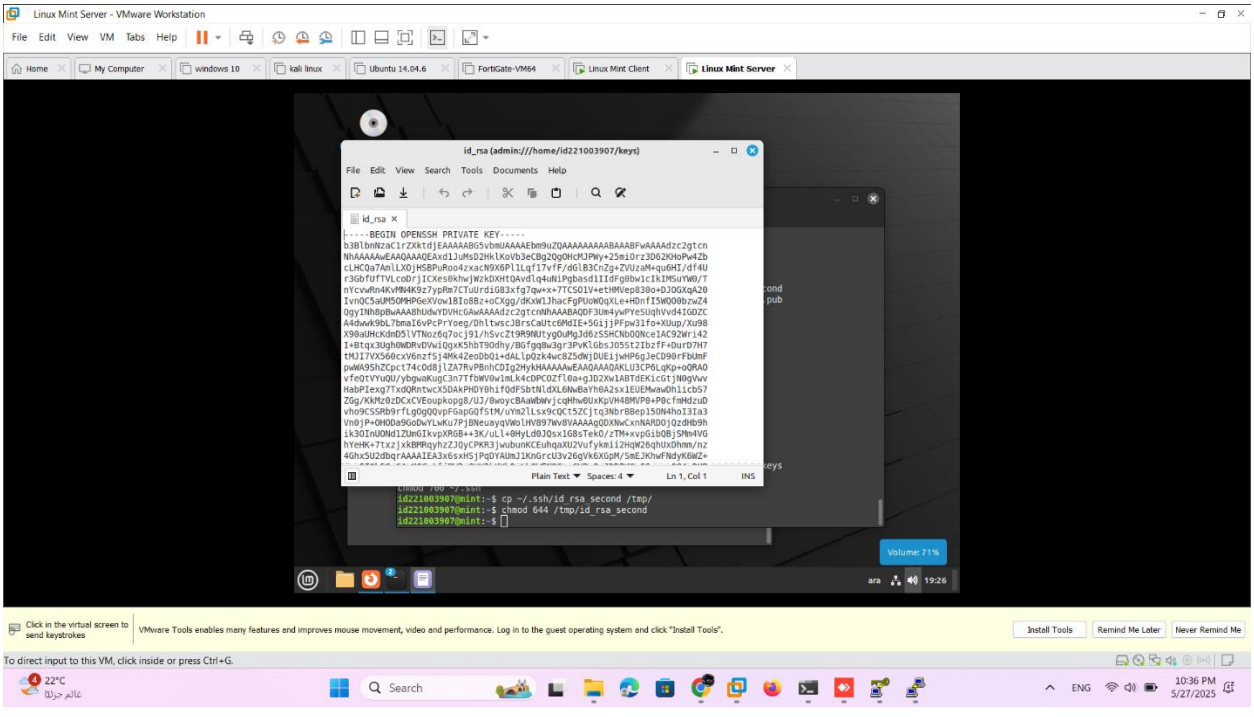
Then try to connect using the key:





Step 6: Generate key pairs on your client and copy the public key file to

server through CLI, then connect using key-pairs.

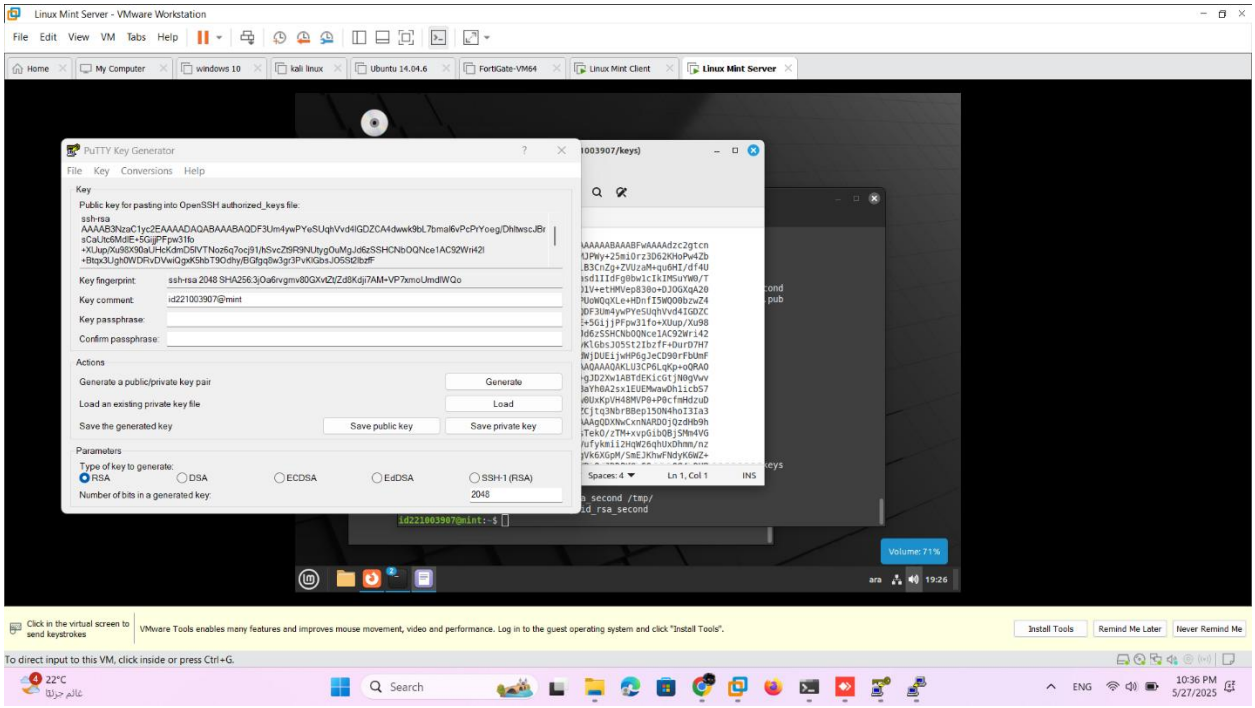


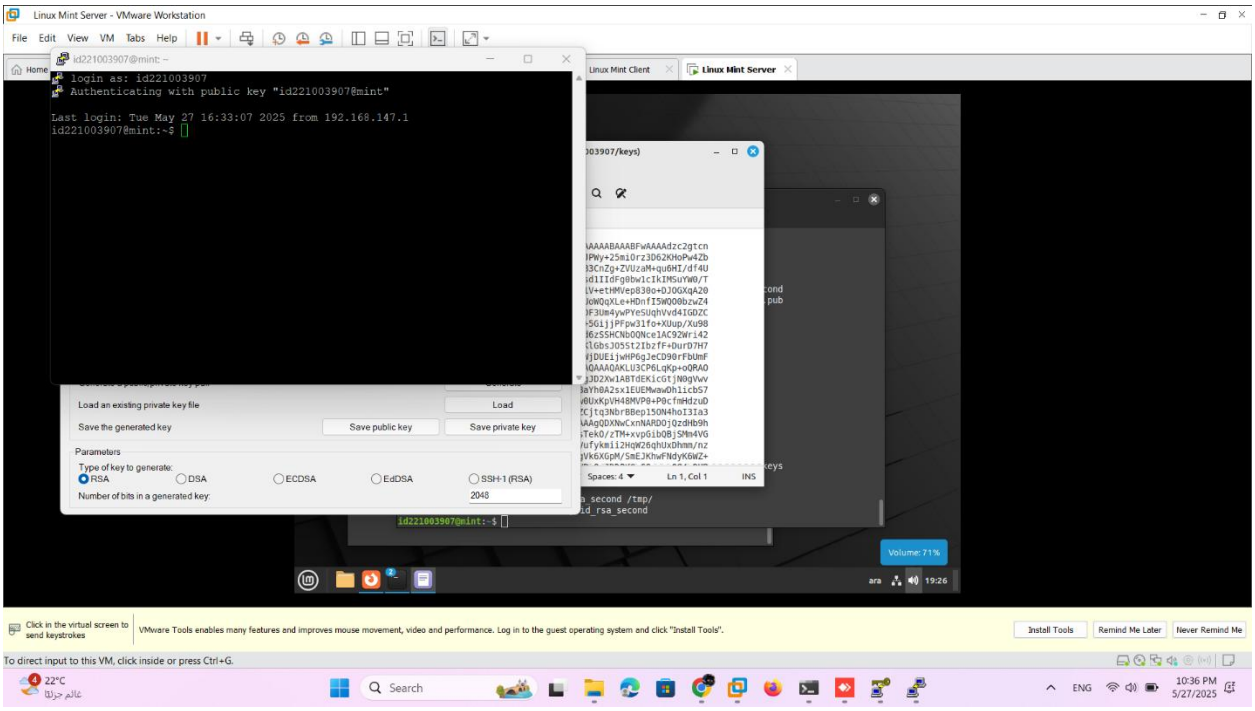
Step 7 :Access Linux Server from Windows using PuTTY and RSA Key

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.**

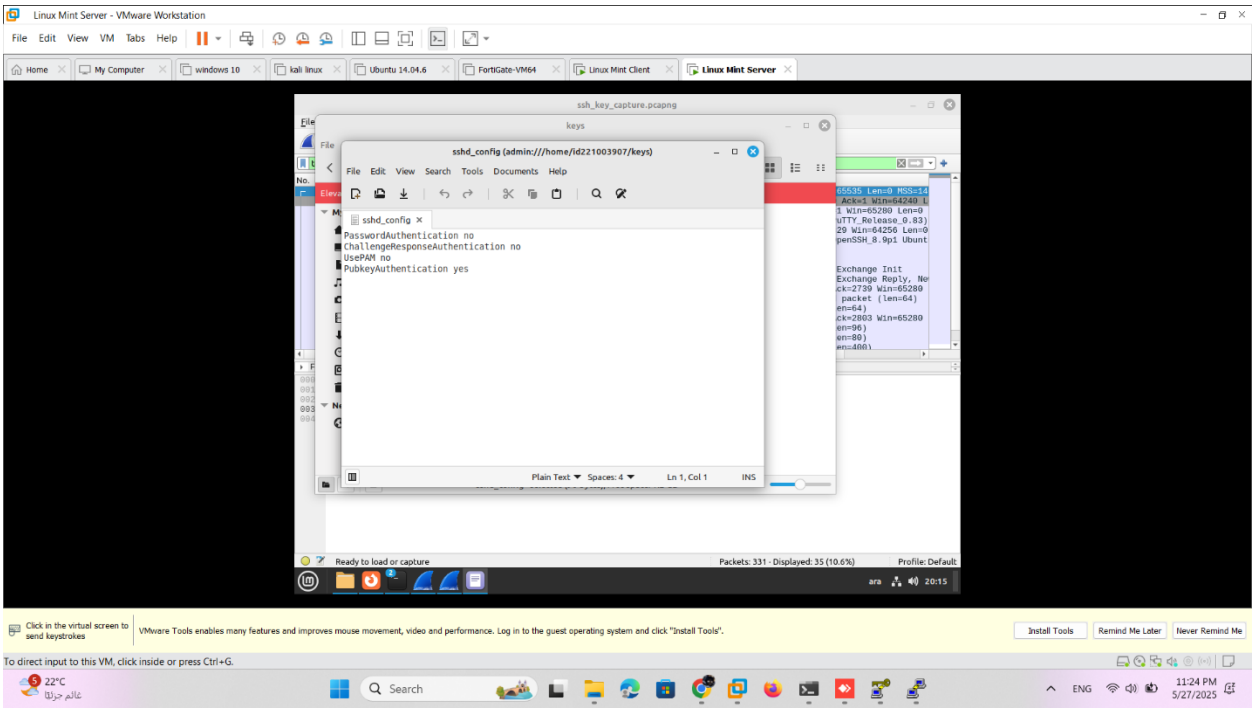
- **Use PuTTY to connect with the key:**
- **Open PuTTY.**
- **In the Host Name field:**
  192.168.147.131
- **Port:22**
- **Go to:**
  Connection > SSH > Auth
- **In the field: Private key file for authentication, browse and select your saved file:**
  id_rsa_windows.ppk





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**