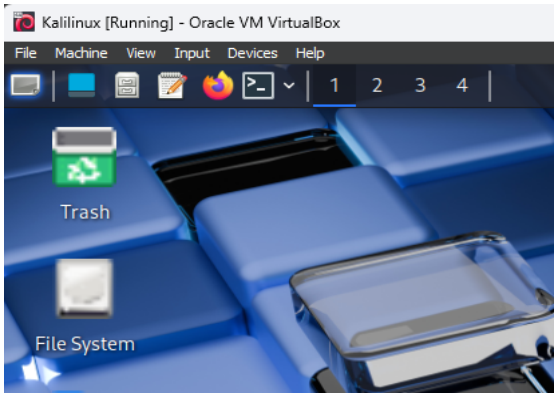
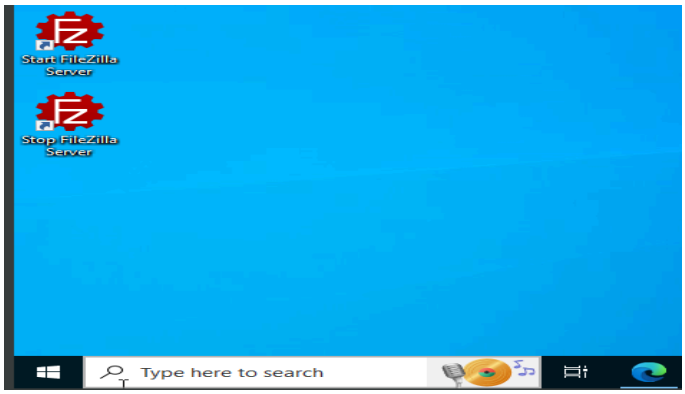
Wireshark Network Traffic Analysis

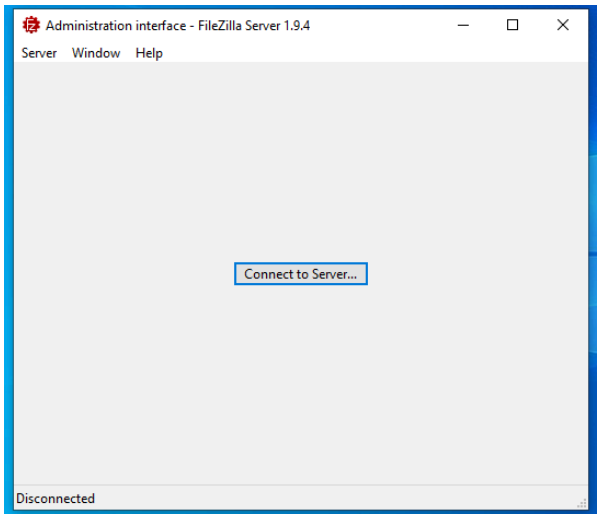




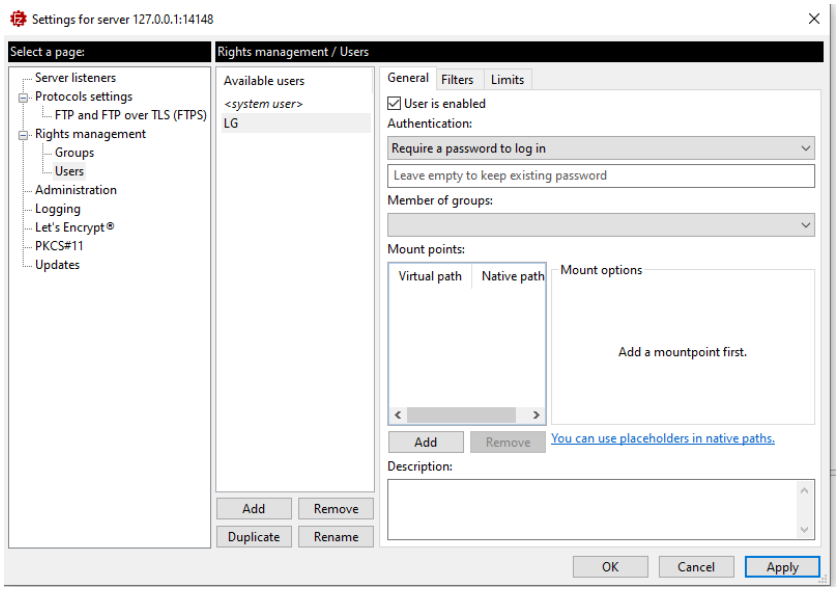
Run **Kali Linux and Windows 10** at the same time using **VirtualBox**. If you haven't set it up yet, install **VirtualBox**, create VMs for both **Kali and Windows 10**, and complete the OS installation. Make sure to allocate enough **RAM and storage** for smooth performance. Set both **VMs to "Bridged Adapter"** in **VirtualBox Network Settings** to allow communication between them.

Step 2: On your **Windows 10 Virtual Machine**, open your browser and search for **FileZilla Server**. Go to the **official FileZilla website** and

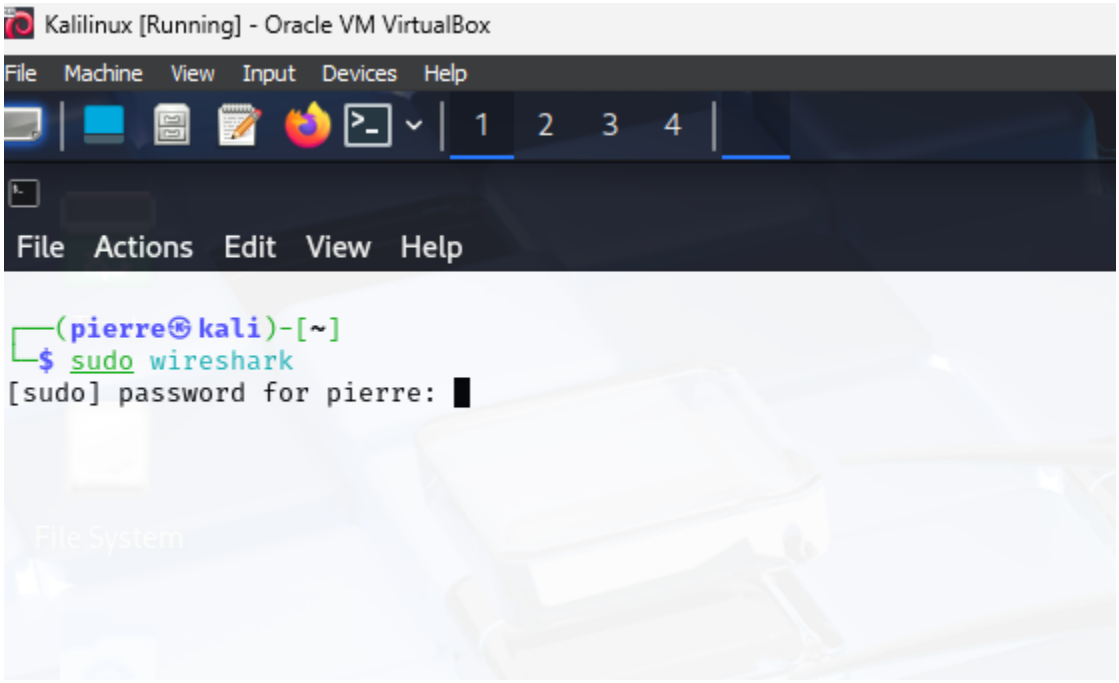
download the **FileZilla Server** for Windows. Click the download button to get the installer.



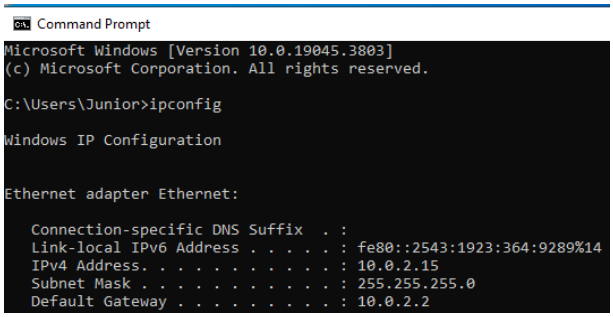
Step 3: Once **FileZilla Server** is downloaded, open it and click **"Connect to Server"**, then click **"OK"** to proceed.



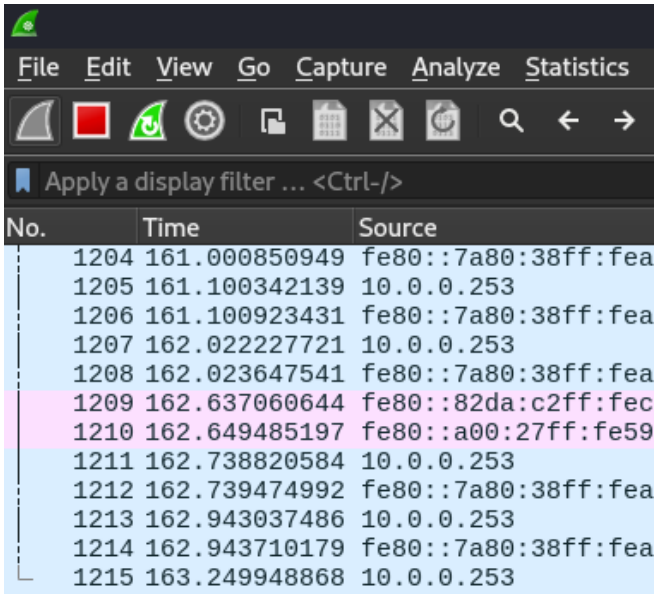
Step 4: Click on the **Server** tab in the top left, then select **Users**. Click **"Add"** at the bottom and enter a username and add a password . Once done, click **"Apply"** and then **"OK"** to save the settings.



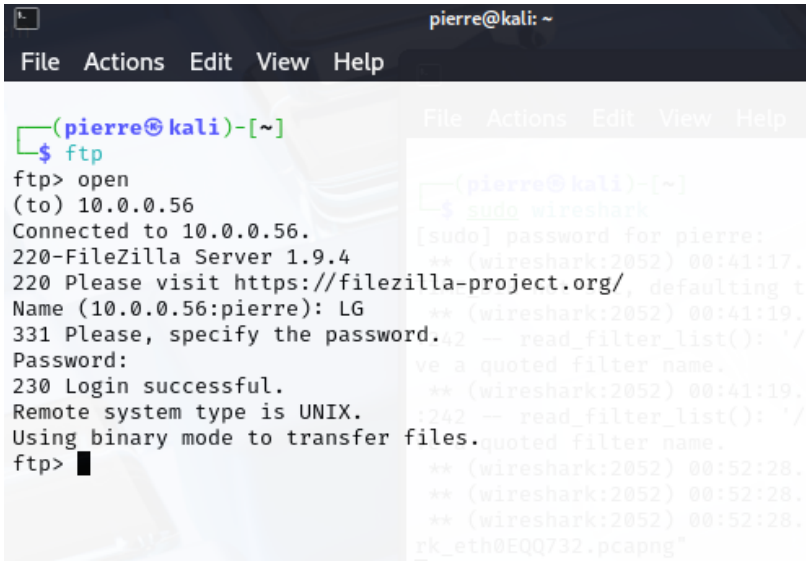
Step 5: On your **Kali Linux virtual machine**, open the terminal and run `sudo wireshark`. Since Wireshark is pre-installed, it will launch without needing to download it.



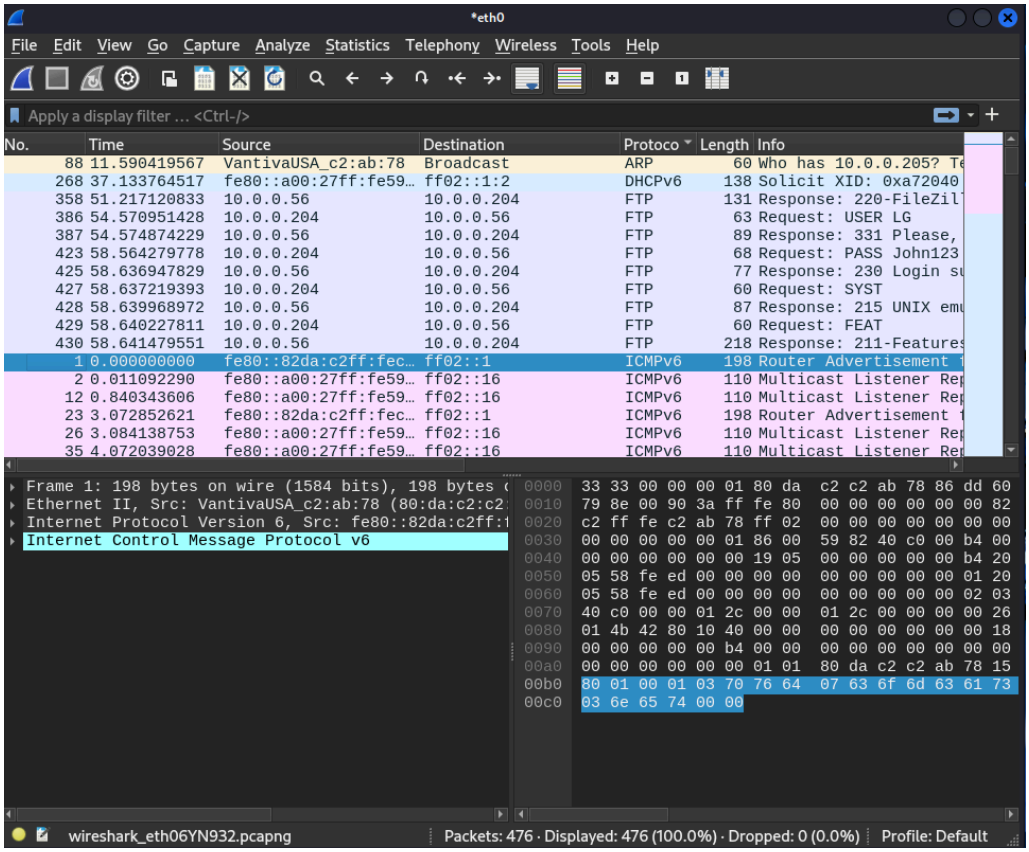
Step 6: Go back to your **Windows 10 virtual machine** and open the **Command Prompt**. Type `ipconfig` to find the **IP address** of the Windows machine.



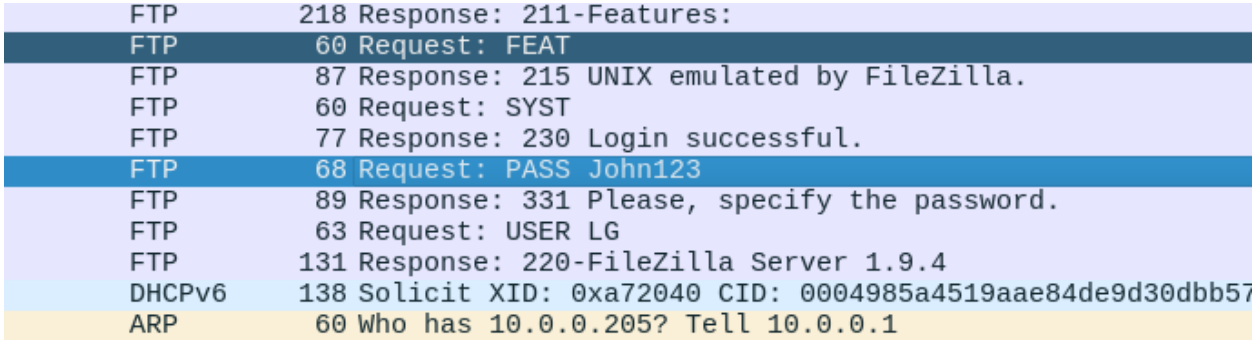
Step 8: Now, on **Wireshark in Kali**, click on the **blue shark fin** icon in the top left to start capturing **packets**.



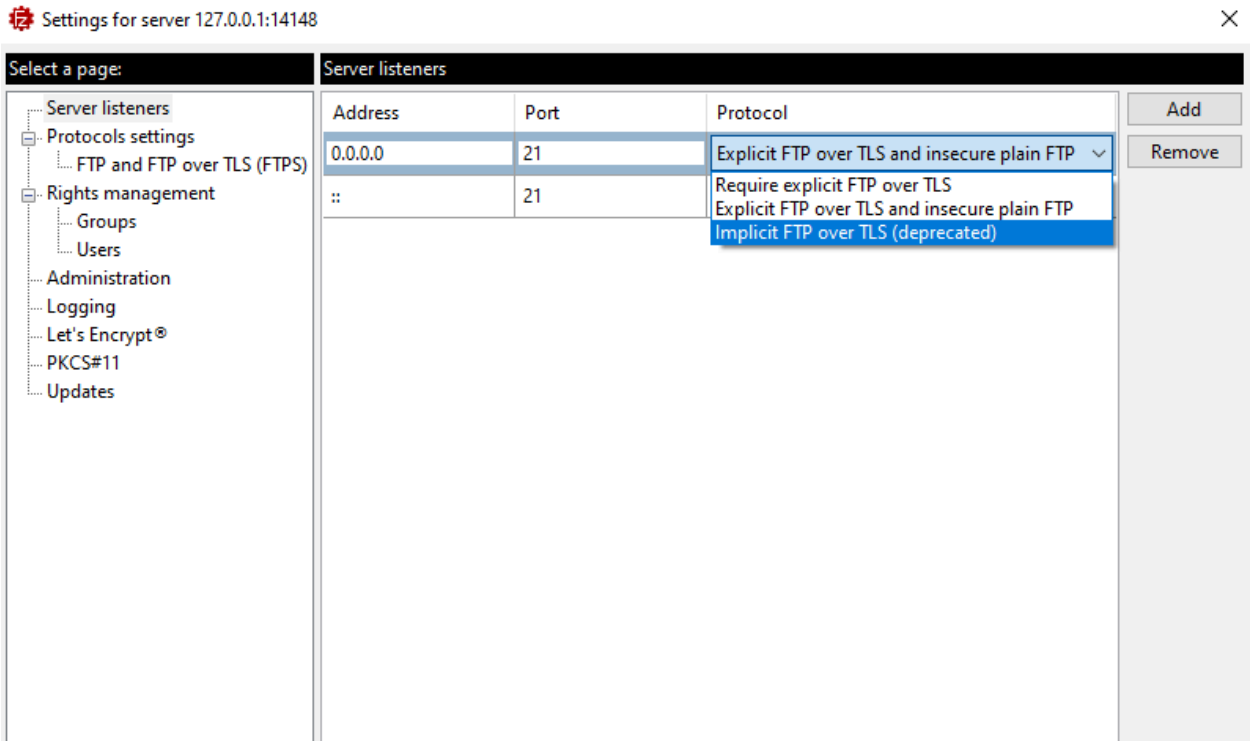
Step 9: Open the terminal and type `ftp`, then **open** followed by your Windows **IPv4 address**. When prompted, enter your **FileZilla username** and **password**. If the login is successful, you're now connected to the FTP server.



Step 10: Go back to **Wireshark** after successfully logging in, then click the **square stop button** to pause the packet capture. Click the **protocol dropdown** at the top, and select the protocol you want to focus on, in this case, **FTP**.



Step 11: As you can see, my **username and password** are exposed. This is why you **shouldn't use FTP (port 21)** . Anyone sniffing the network can steal your credentials. Instead, use **SFTP (port 22)** for secure, encrypted file transfers.



Step 12; You can use **Wireshark** to confirm that **plain FTP does not encrypt usernames and passwords**, making them visible to anyone sniffing the network. To secure your connection, go to **FileZilla Server** and configure it to **require FTPS (FTP over TLS)** instead of plain FTP. In the **server listeners** area, under **protocol**, select **Explicit FTP over TLS** instead of **Plaintext** to encrypt your data and protect your credentials..

Step 13: Close All Tabs to End the Project