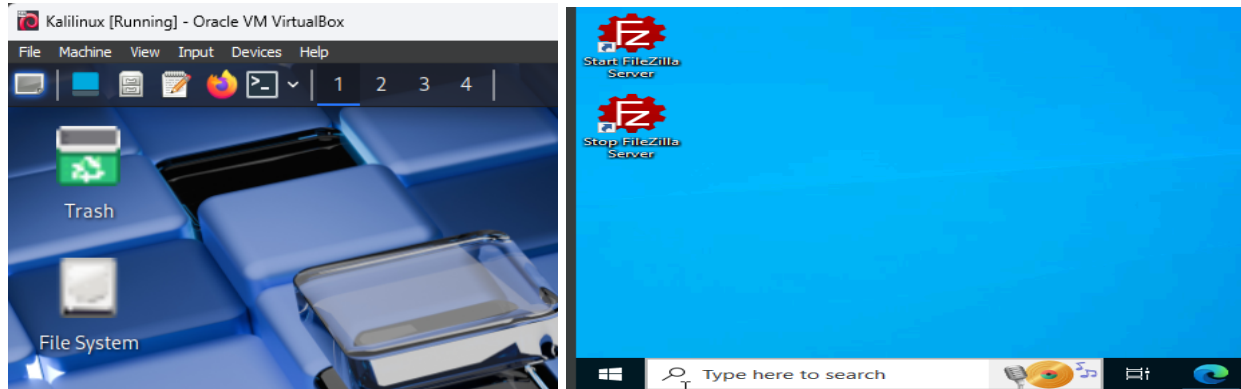


Wireshark Network Traffic Analysis

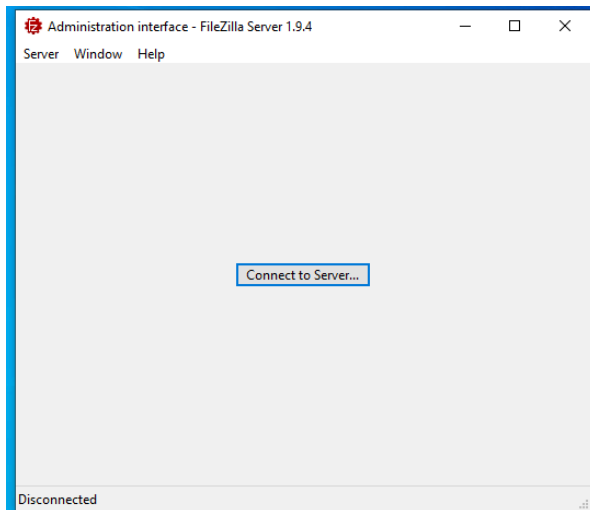


Step 1: Run Kali Linux and Windows 10 at the same time using VirtualBox. If you haven't set it up yet, install **VirtualBox**, create VMs for both **Kali** and **Windows 10**, and complete the OS installation. Make sure to allocate enough **RAM** and **storage** for smooth performance. Set both **VMs** to "**Bridged Adapter**" in **VirtualBox Network Settings** to allow communication between them.

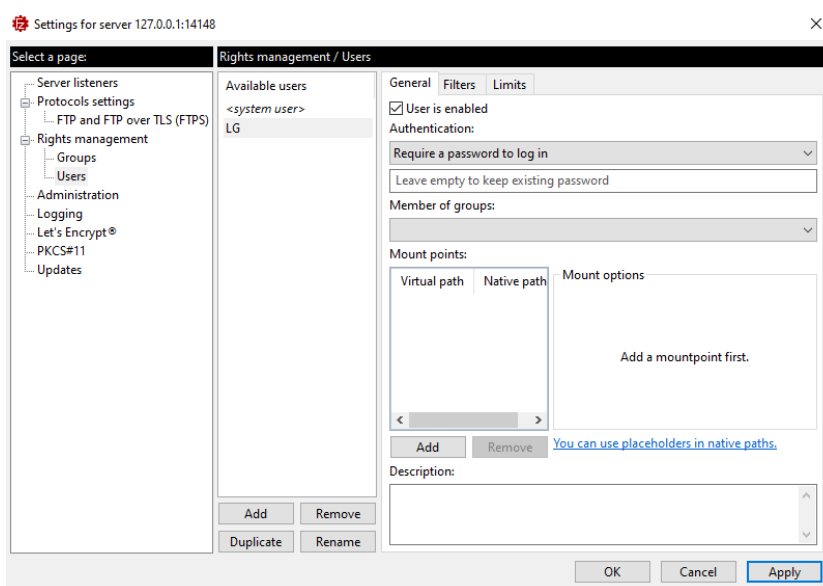


Step 2: On your Windows 10 Virtual Machine, open your browser and search for FileZilla Server. Go to the official FileZilla website and

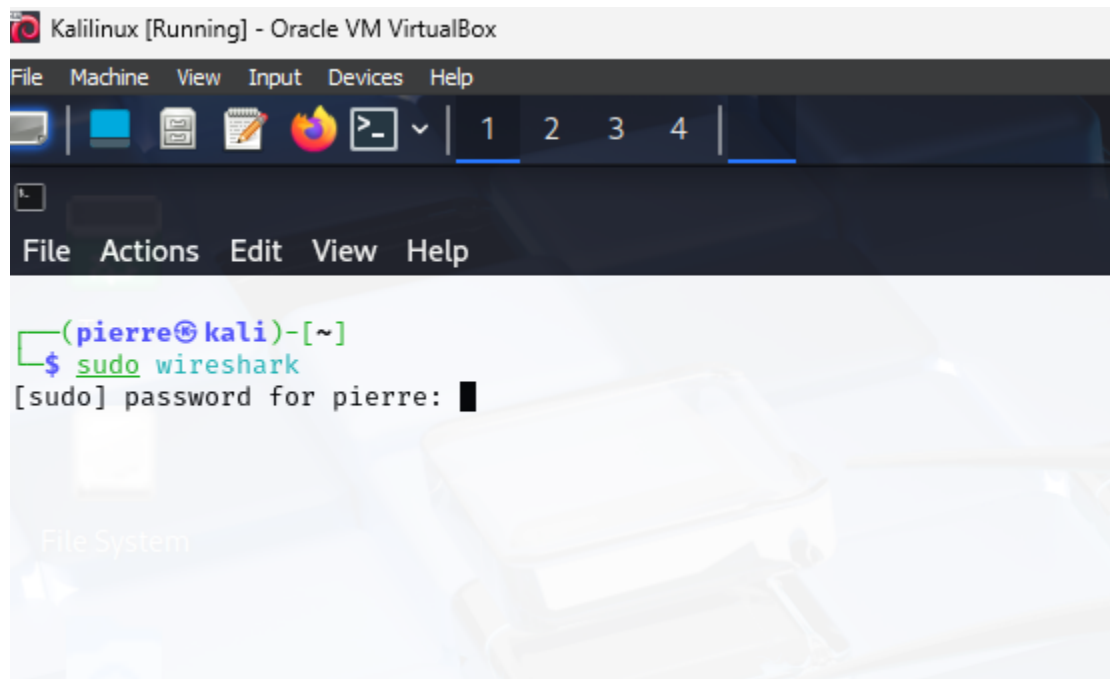
download the **FileZilla Server** for Windows. Click the download button to get the installer.



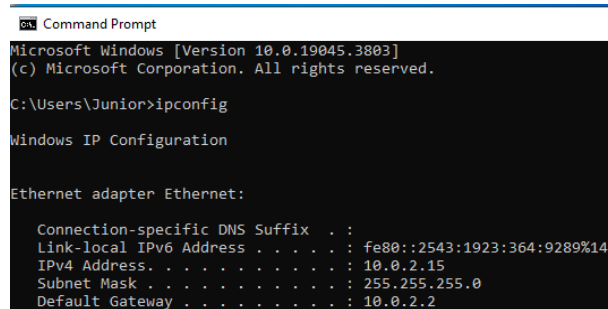
Step 3: Once **FileZilla Server** is downloaded, open it and click "**Connect to Server**", then click "**OK**" to proceed.



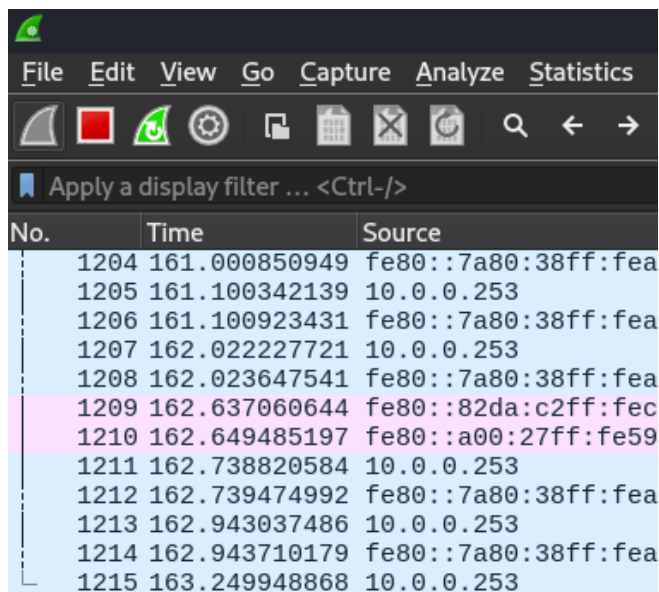
Step 4: Click on the **Server** tab in the top left, then select **Users**. Click "**Add**" at the bottom and enter a username and add a password . Once done, click "**Apply**" and then "**OK**" to save the settings.



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.

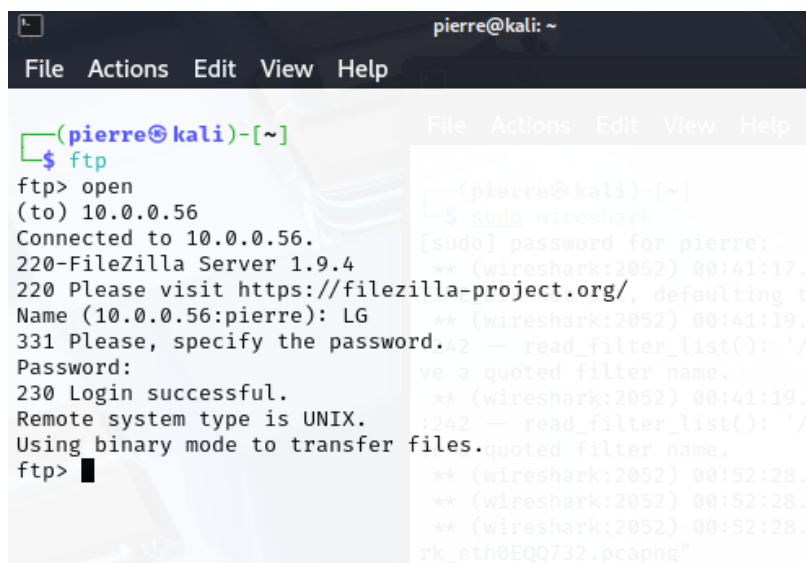


Step 6: Go back to your **Windows 10 virtual machine** and open the **Command Prompt**. Type `ipconfig` to find the **IP address** of the Windows machine.



No.	Time	Source
1204	161.000850949	fe80::7a80:38ff:fea
1205	161.100342139	10.0.0.253
1206	161.100923431	fe80::7a80:38ff:fea
1207	162.022227721	10.0.0.253
1208	162.023647541	fe80::7a80:38ff:fea
1209	162.637060644	fe80::82da:c2ff:fec
1210	162.649485197	fe80::a00:27ff:fe59
1211	162.738820584	10.0.0.253
1212	162.739474992	fe80::7a80:38ff:fea
1213	162.943037486	10.0.0.253
1214	162.943710179	fe80::7a80:38ff:fea
1215	163.249948868	10.0.0.253

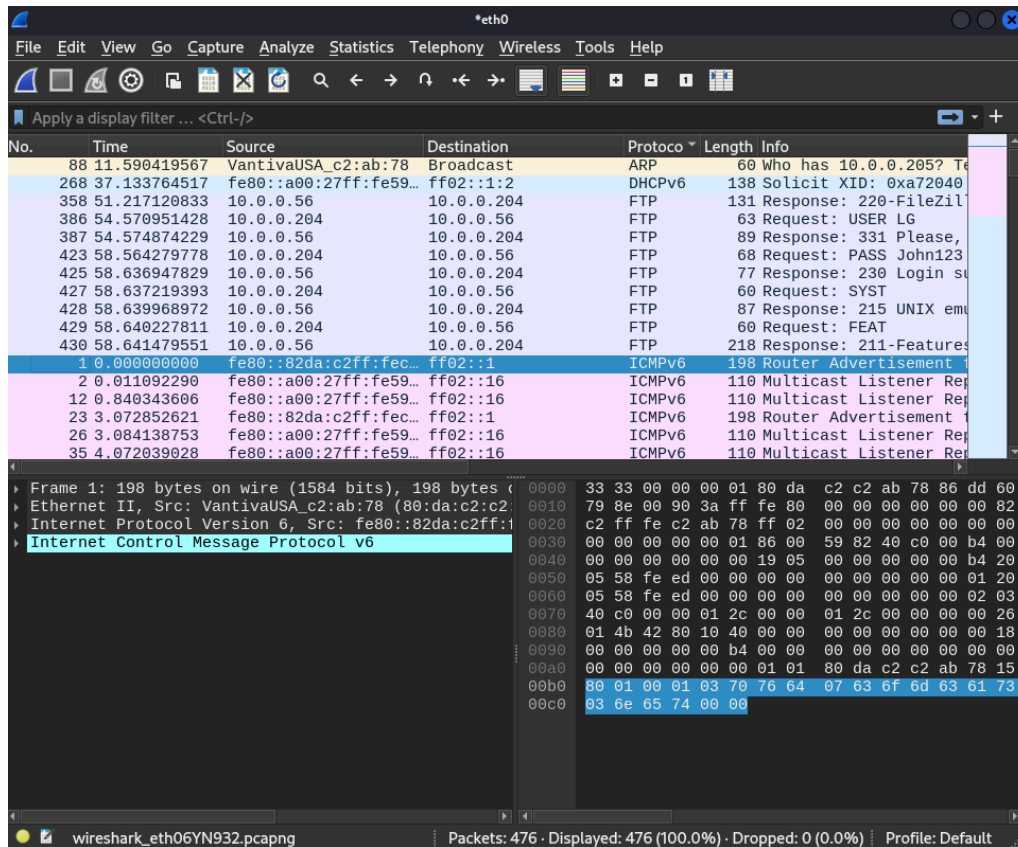
Step 8: Now, on **Wireshark** in **Kali**, click on the **blue shark fin** icon in the top left to start capturing **packets**.



```
pierre@kali: ~
File Actions Edit View Help

(pierre@kali)-[~]
$ ftp
ftp> open
(to) 10.0.0.56
Connected to 10.0.0.56.
220-FileZilla Server 1.9.4
220 Please visit https://filezilla-project.org/
Name (10.0.0.56:pierre): LG
331 Please, specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

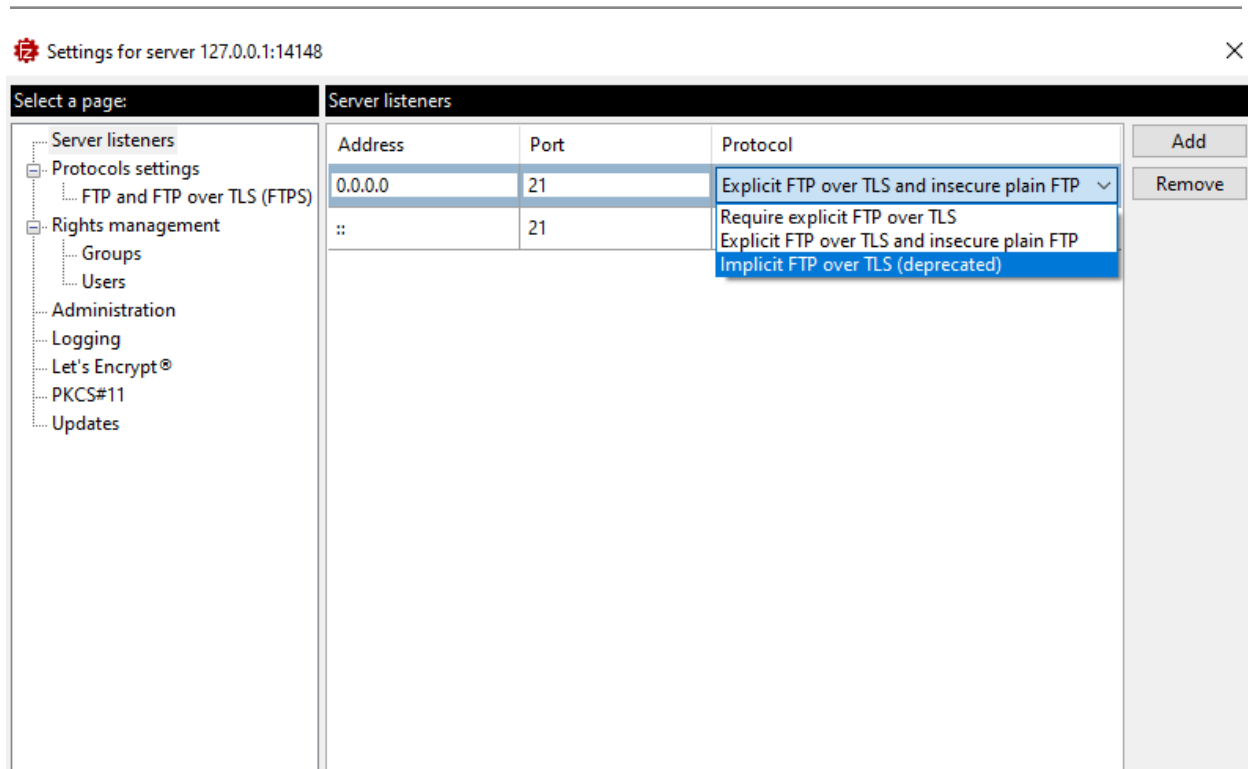
Step 9: Open the terminal and type **ftp**, then **open** followed by your Windows **IPv4 address**. When prompted, enter your **FileZilla username** and **password**. If the login is successful, you're now connected to the FTP server.



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**.

FTP	218 Response: 211-Features:
FTP	60 Request: FEAT
FTP	87 Response: 215 UNIX emulated by FileZilla.
FTP	60 Request: SYST
FTP	77 Response: 230 Login successful.
FTP	68 Request: PASS John123
FTP	89 Response: 331 Please, specify the password.
FTP	63 Request: USER LG
FTP	131 Response: 220-FileZilla Server 1.9.4
DHCPv6	138 Solicit XID: 0xa72040 CID: 0004985a4519aae84de9d30dbb57
ARP	60 Who has 10.0.0.205? Tell 10.0.0.1

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