

Conestoga College

Course	INF08965 - Network and Security
Activity Title	Internet Traffic Analysis
Student Name	Twinkle Akhilesh Mishra
Student Number	8894858
Lab performed on (Date):	27-Jan-2025

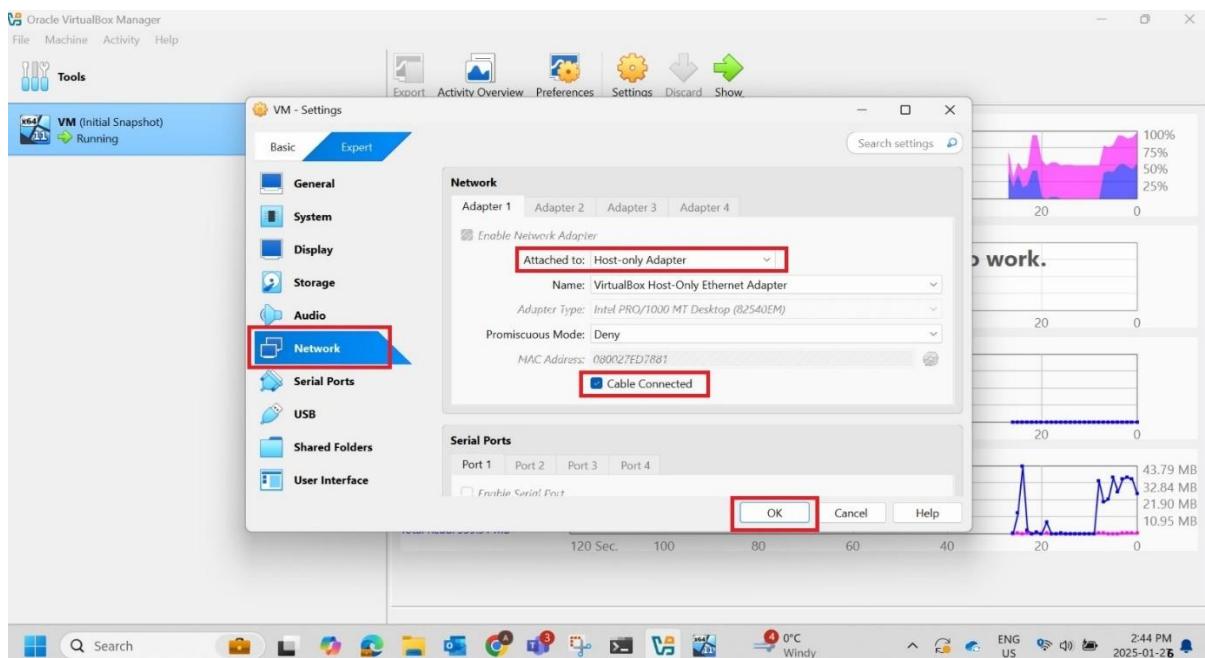
Objectives

- Analyse network traffic using traffic capture utility like Wireshark.**
- Setup an FTP server in a Virtual Machine**
- For IP addressing in this lab, XY (58) represents the last two digits of your student ID.**

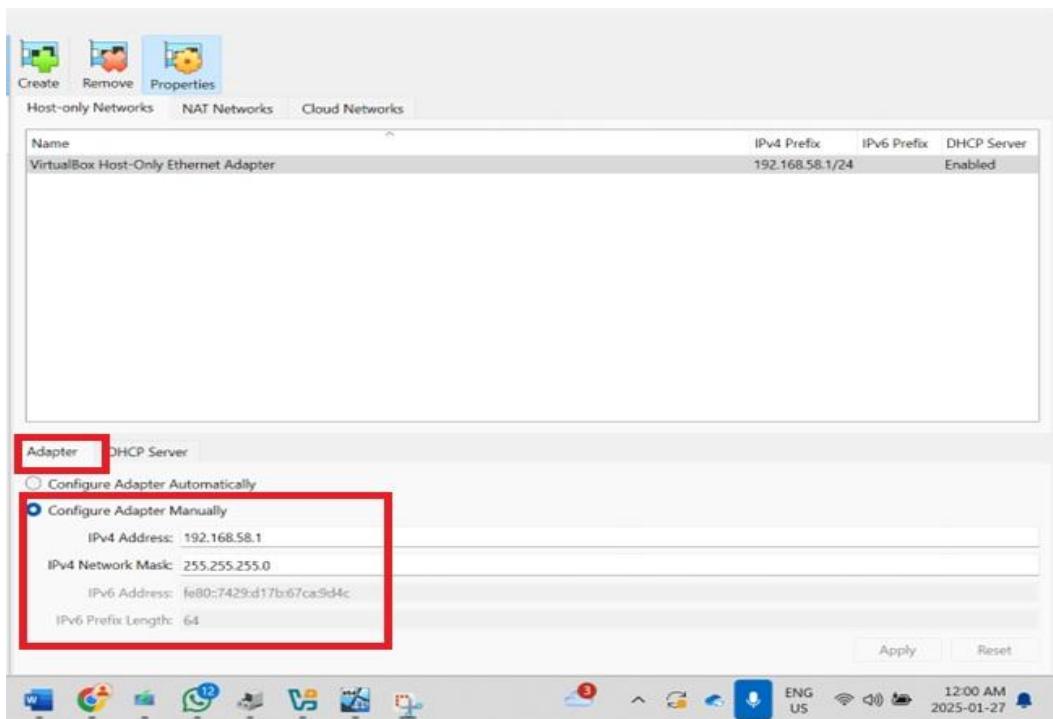
Step 1: Install and Run FTP Server

1. Configure Host-Only Adapter:

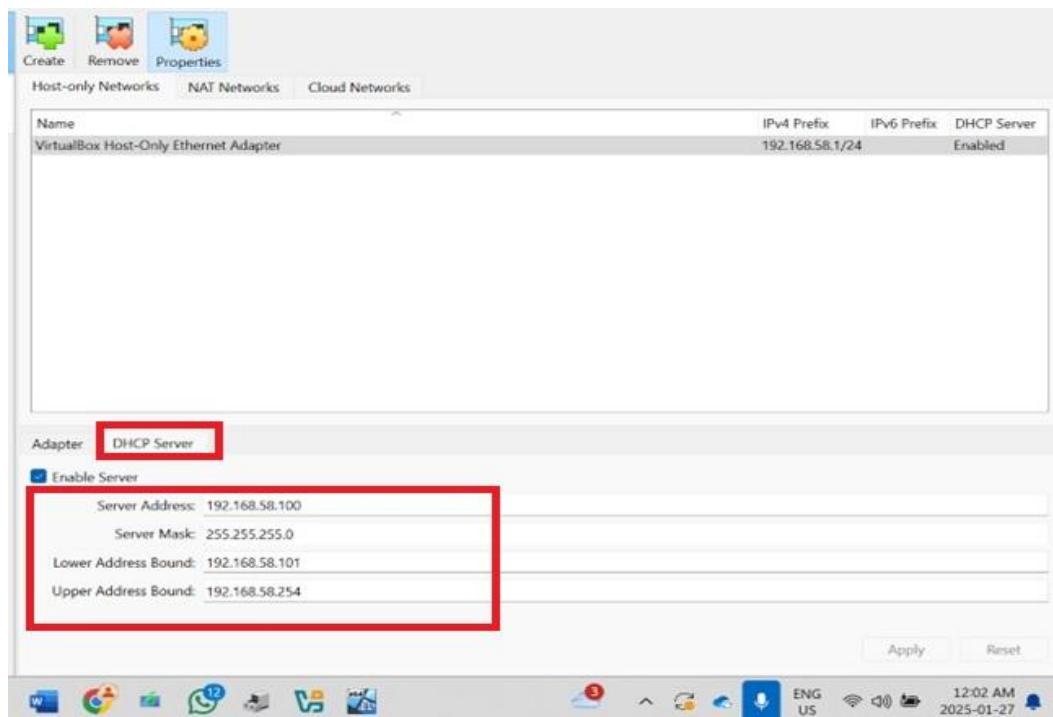
- Using VirtualBox, created a **Host-Only Ethernet Adapter**.
- Given the IP address **192.168.58.1** and the network mask **255.255.255.0**.
- Setup **DHCP** server with IP address **192.168.58.100**
- Lower/upper bounds: **192.168.58.101 - 192.168.58.254**



- **Change Adapter IP to .58:**

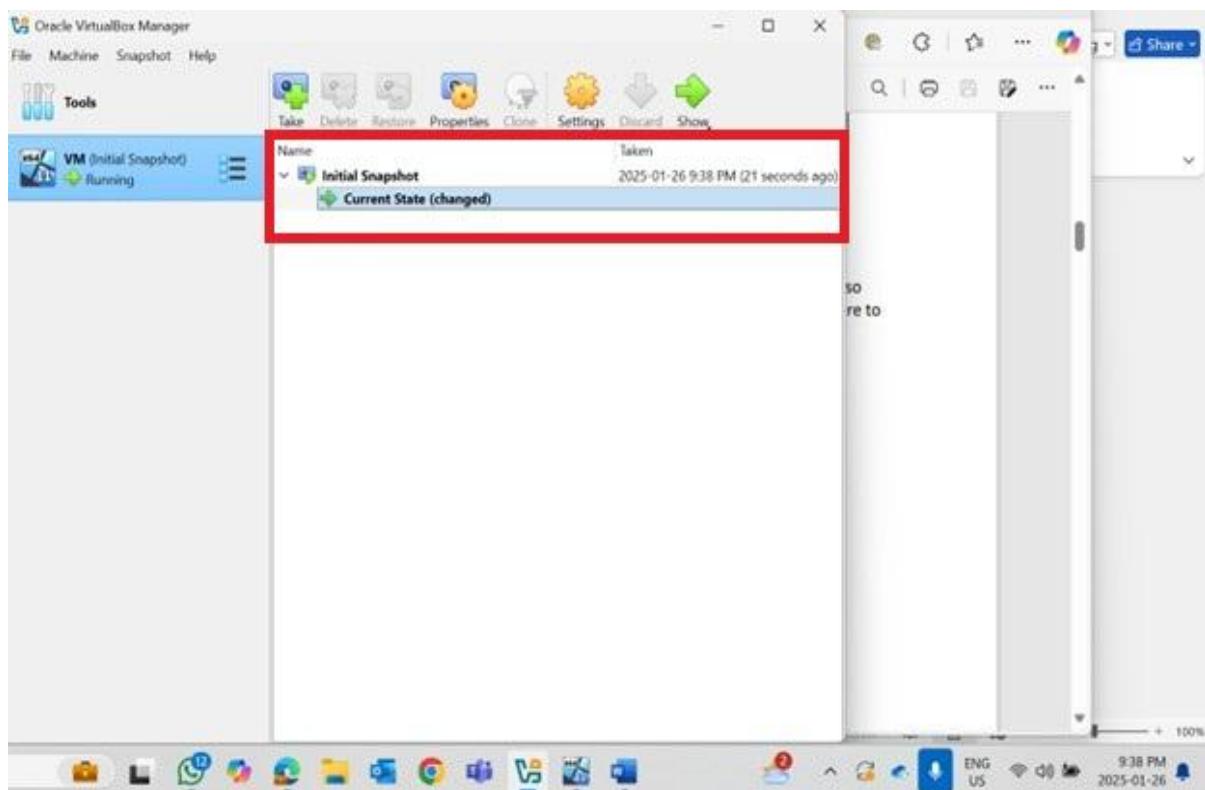
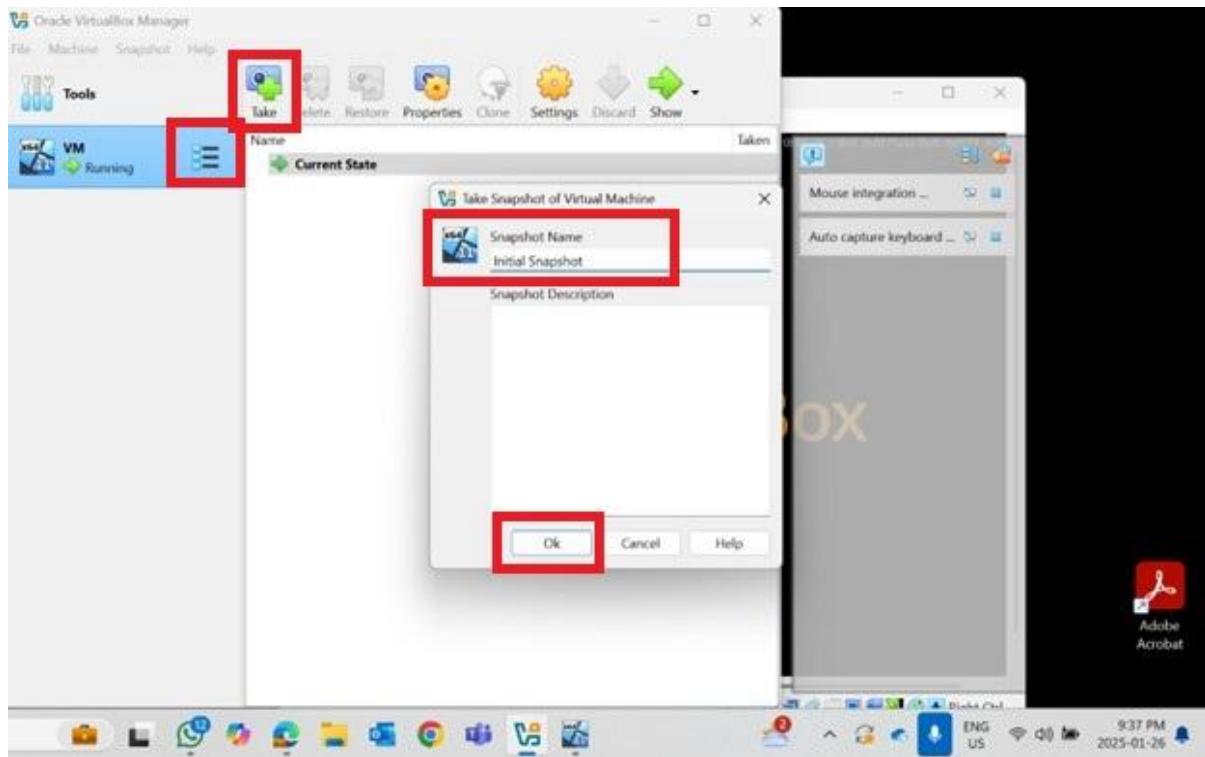


- **Change DHCP Server to .58**



2. Take a Snapshot:

- Created an initial snapshot of the Windows 10 VM for backup.

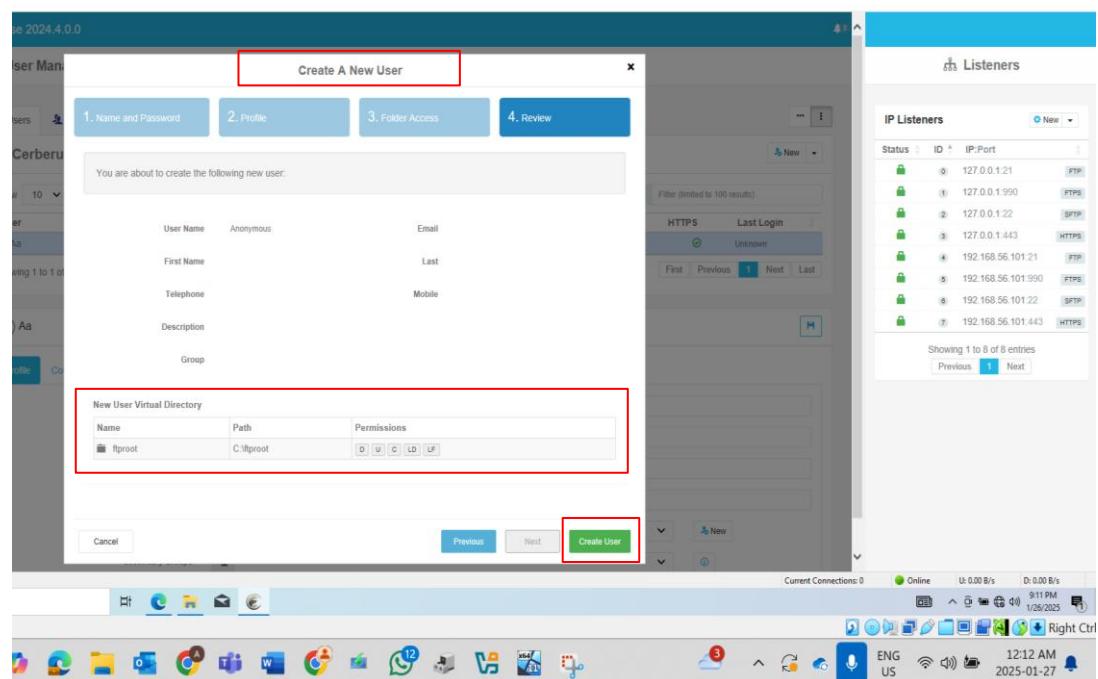
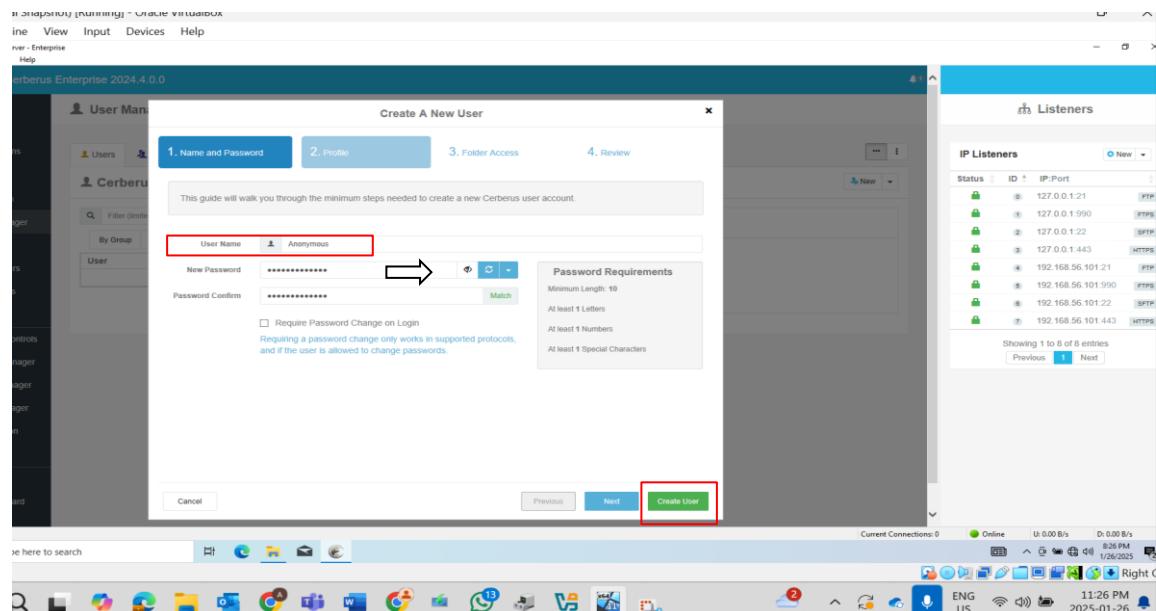


3. Install Cerberus FTP Server:

- Installed Cerberus on the VM with default settings.
- Allowed unencrypted FTP traffic and disabled SSL/TLS.
- Set up the Anonymous user with a password.
- Verified the FTP server IP address.

4. Create and Test File:

- Created a text file named after Cerberus in C:\ftproot.



- Checked the box for FTP to not allow unsecured FTP server connections

The screenshot shows the Cerberus Enterprise 2024.4.0.0 interface. On the left, the navigation menu is visible with 'User Manager' selected. In the center, the 'Cerberus Users' table shows two entries: 'Anonymous' and 'Aa'. The 'Anonymous' row is highlighted with a red box. A modal window for 'Anonymous' is open, showing the 'Allowed Protocols' tab. This tab contains sections for 'Permitted Login Protocols' and 'FTP Only Settings'. Under 'Permitted Login Protocols', 'Allow FTP' and 'Allow SFTP' are checked, while 'Allow HTTP' and 'Allow HTTPS' are unchecked. Under 'FTP Only Settings', 'Require Secure Control' and 'Require Secure Data' are unchecked. At the bottom of the modal, there is a 'Change Password' button and a blue 'Update User' button, which is also highlighted with a red box. To the right, a 'Listeners' panel shows a table of IP listeners with columns for Status, ID, IP:Port, and Protocol. The table lists various listeners including FTP, SFTP, and HTTPS. The status column shows green locks for most entries.

- Disable secure control and data

The screenshot shows the Cerberus Enterprise 2024.4.0.0 interface. On the left, the navigation menu is visible with 'Server Manager' selected. In the center, a 'New FTP Defaults' configuration dialog is open. It has tabs for 'General', 'Security', and 'Advanced'. The 'General' tab is active, showing 'Default Port: 21'. Under 'Security', the 'Allow Login' checkbox is checked and highlighted with a red box. Below it, 'Port' is set to 21 and 'Connection Limit' is set to 500. Under 'FTP Security', 'Require Secure Control' and 'Require Secure Data' checkboxes are present but unchecked. The 'Advanced' tab contains sections for 'FTP Passive Mode' (with options like 'Auto Detect', 'Use Different IP for Passive', and 'Use a DNS Service') and 'DNS Resolution' (with a note about specifying a DNS address). At the bottom, there is a 'Save' button and a 'Cancel' button. To the right, a 'Listeners' panel shows a table of IP listeners with columns for Status, ID, IP:Port, and Protocol. The table lists various listeners including FTP, SFTP, and HTTPS. The status column shows green locks for most entries.

■ Disable SSL/TLS

The screenshot displays the Cerberus Enterprise 2024.4.0.0 interface. On the left, a sidebar lists various management sections like Summary, Log, Connections, Reporting, Authentication, User Manager, AD Users, LDAP Users, SSO Users, Configuration, Firewall Controls, and Server Manager. The Server Manager section is currently selected and highlighted with a red box. The main content area shows the 'Security' tab, which has several sub-tabs: General, Advanced TLS, 2FA, Server Verification, and Client Verification. The 'General' sub-tab is active and has a red box around its 'Enable SSL/TLS' checkbox. Below this, a note states: 'Disabling TLS is not recommended and will result in FTPS, SSH SFTP, and HTTPS failures.' A 'TLS Server Key Pair' section displays certificate details: Subject (CN=DESKTOP-8POBC71, O=Cerberus FTP Server, OU=Self-signed Certificate, C=US), Self Signed Certificate (Yes), Key Type (RSA (2048)), Issued (01/26/2025), Expires (01/26/2028), Certificate Path (C:\ProgramData\cerberus LLC\cerberus FTP Server\certificates\server.pem), and Private Key Path (C:\ProgramData\cerberus LLC\cerberus FTP Server\certificates\server.pem). The 'Listeners' panel on the right lists eight IP listeners with their respective statuses, IP addresses, and port numbers. The listeners include various protocols such as FTP, SFTP, and HTTPS.

▪ **Setting password for Anonymous user:**

The screenshot shows the Cerberus Server interface. On the left, a 'Change Password' dialog is open, prompting for a new password ('New Password') and its confirmation ('Password Confirm'). A red box highlights the 'New Password' field and the 'Match' button. To the right of the dialog is a 'Listeners' list table. The table has columns for Status, ID, IP:Port, and Type. It lists several entries, with a red box highlighting the row for port 10121 (Type: FTP). The bottom of the screen shows a taskbar with various icons and system status information.

Status	ID	IP:Port	Type
Locked	①	127.0.0.1:21	FTP
Locked	②	127.0.0.1:990	FTPS
Locked	③	127.0.0.1:22	SFTP
Locked	④	127.0.0.1:443	HTTPS
Locked	⑤	192.168.56.101:21	FTP
Locked	⑥	192.168.56.101:990	FTPS
Locked	⑦	192.168.56.101:22	SFTP
Locked	⑧	192.168.56.101:443	HTTPS

▪ **IP address for Cerberus FTP Server:**

The screenshot shows the Cerberus Server interface. On the left, a 'Listeners' list table is displayed. The table has columns for how, ID, IP, Port, Type, and Max Connections. It lists multiple entries, with a red box highlighting the row for port 10121 (Type: FTP). To the right of the table is another 'Listeners' list table, which also shows entries for various ports and protocols. The bottom of the screen shows a taskbar with various icons and system status information.

how	ID	IP	Port	Type	Max Connections
①		New FTP Defaults	21	FTP	500
Locked	②	New FTPS Defaults	990	FTPS	500
Locked	③	New SFTP Defaults	22	SFTP	500
④		New HTTP Defaults	80	HTTP	500
Locked	⑤	New HTTPS Defaults	443	HTTPS	500
⑥		127.0.0.1	21	FTP	500
Locked	⑦	127.0.0.1	990	FTPS	500
Locked	⑧	127.0.0.1	22	SFTP	500
Locked	⑨	127.0.0.1	443	HTTPS	500
⑩		192.168.56.101	21	FTP	500

Step 2: Download File and Capture FTP Traffic

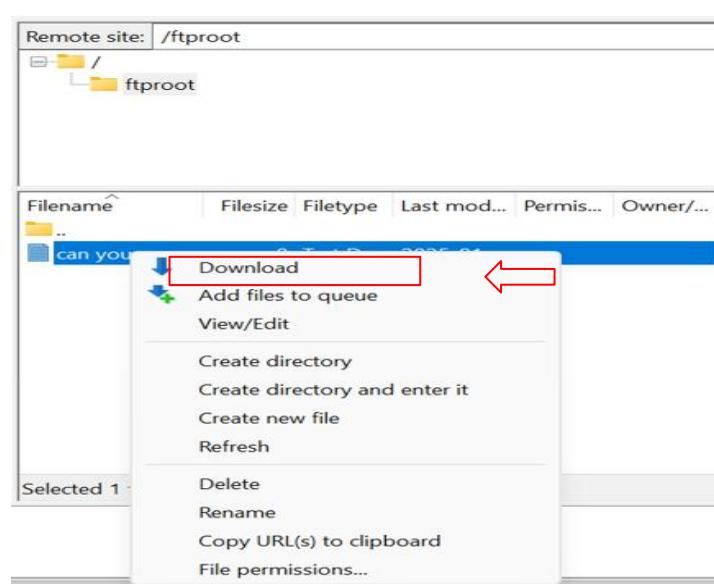
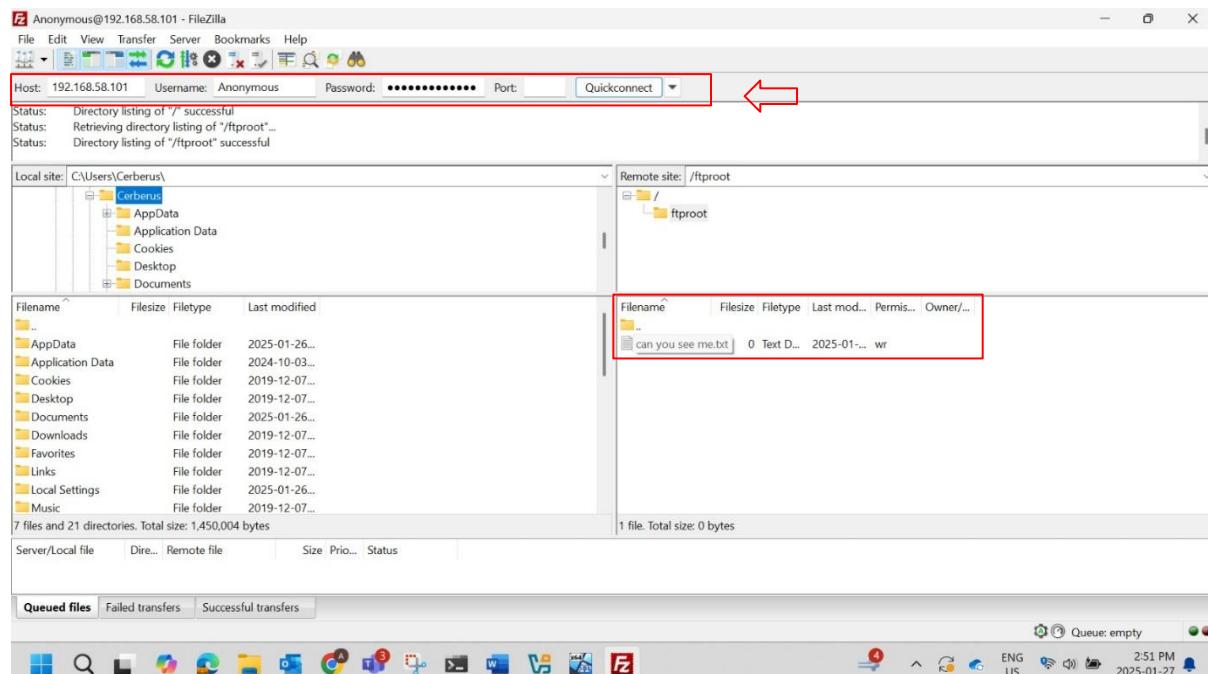
1. Install FileZilla Client:

- Installed FileZilla Client on the host machine.

2. Capture FTP Traffic with Wireshark:

- Started Wireshark on the host and captured traffic on the Host-Only Network.
- Used FileZilla to connect to the FTP server, login, and download the test file.
- Verified server logs in Cerberus.

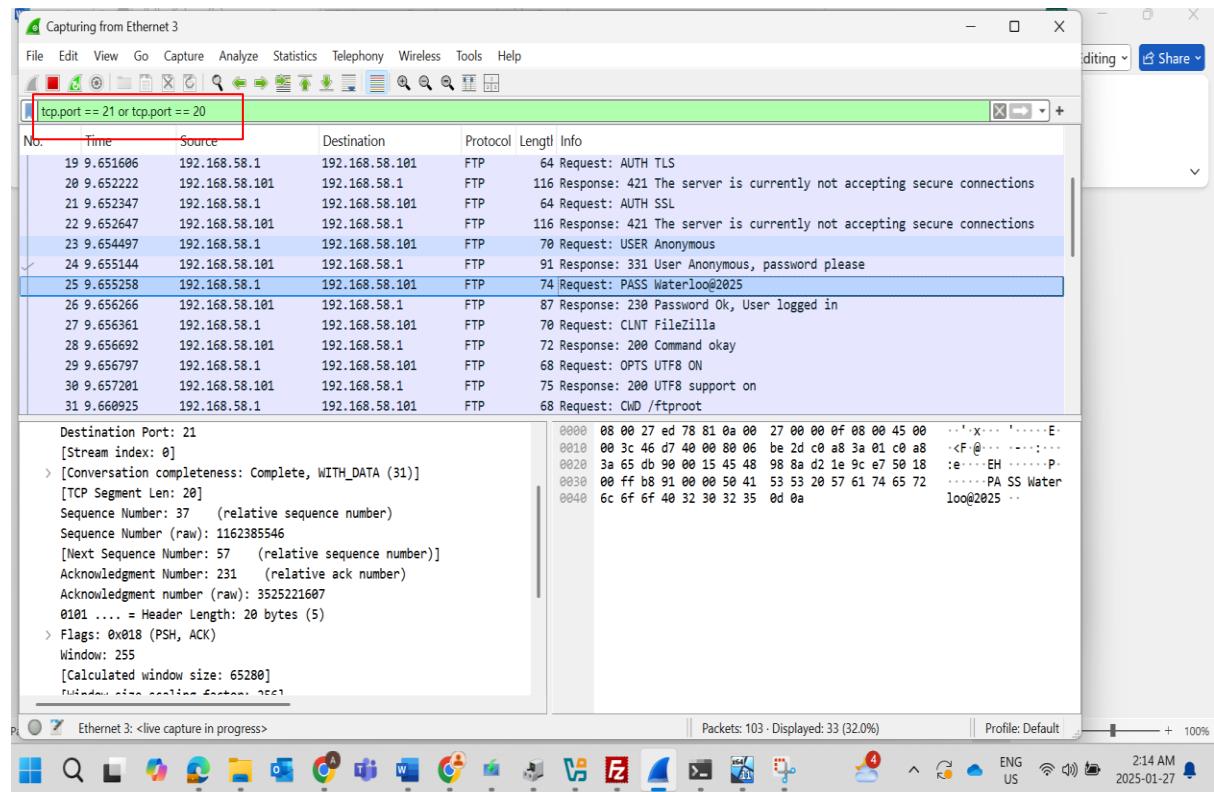
▪ Downloading file hosted on the FTP Server using FileZilla:



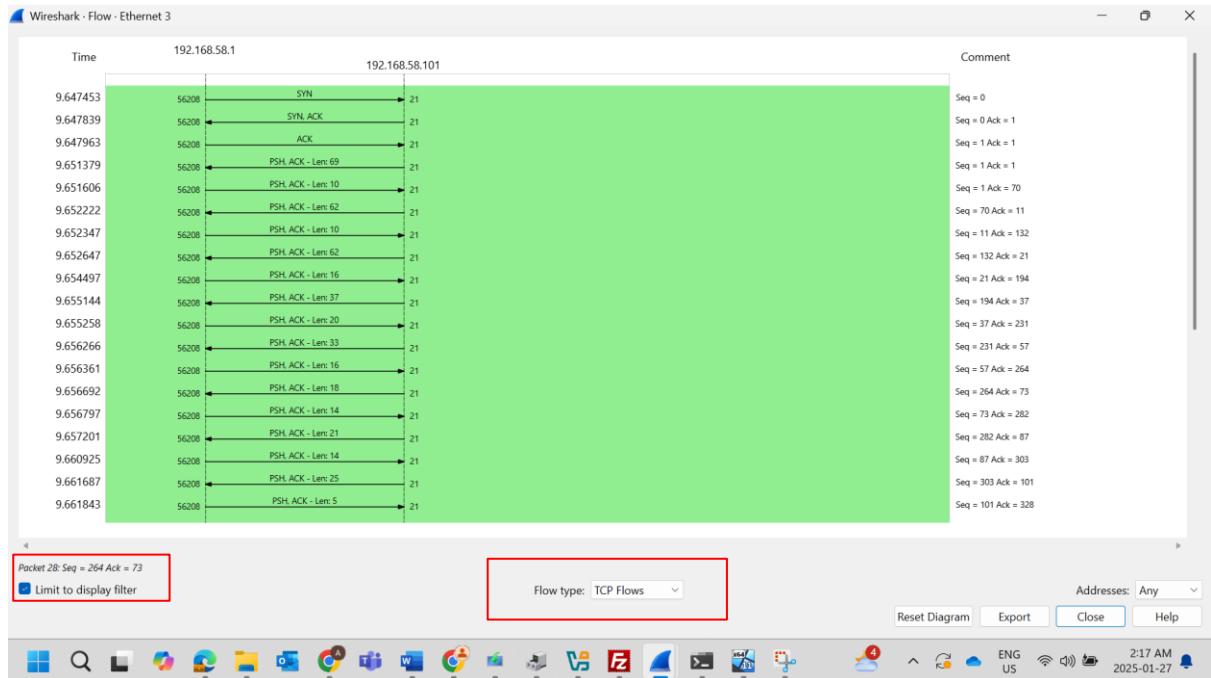
3. Analyze Wireshark Data:

- Applied `tcp.port == 21` or `tcp.port == 20` to display FTP traffic.
- Captured clear-text username and password during login.
- Verified successful 3-way handshakes (SYN, SYN-ACK, ACK).
- Observed file transfer in plain text in captured packets.
- Visualized communication and handshakes between client and server.

Output #1: Apply filter to view only FTP related traffic



Output #2: Flow graph in Wireshark



Output#3: Wireshark Capture of File Transfer in Clear Text

