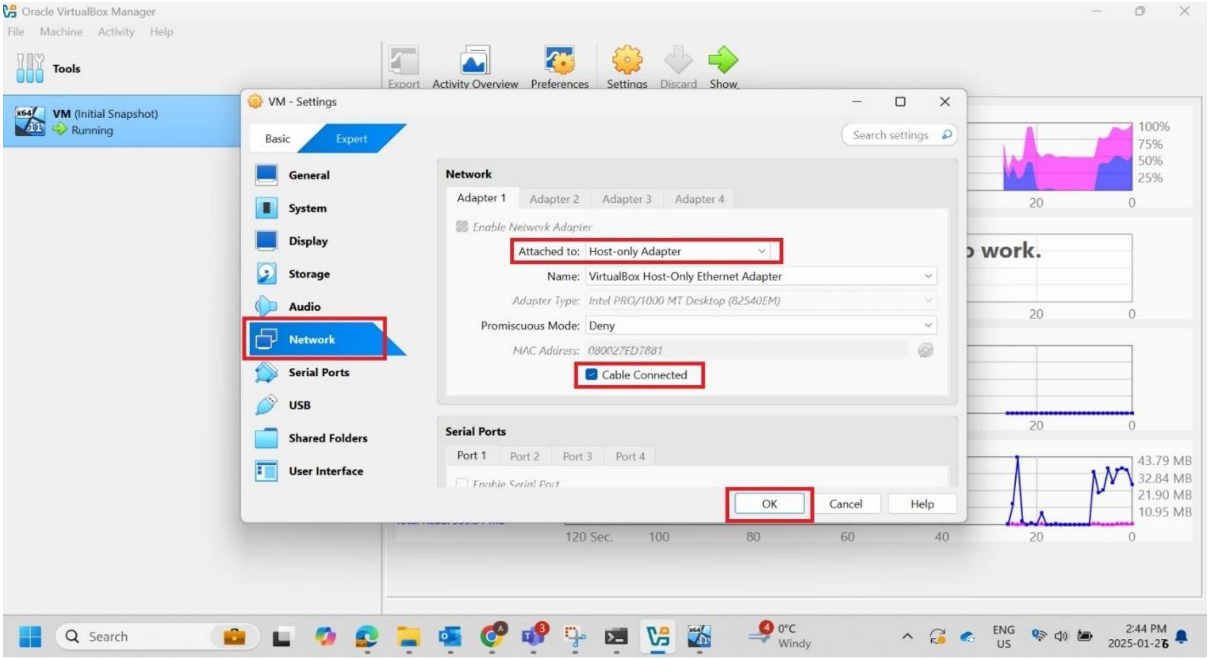
Conestoga College

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 launch the 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**



VM - Settings

Network — Adapter 1

□ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

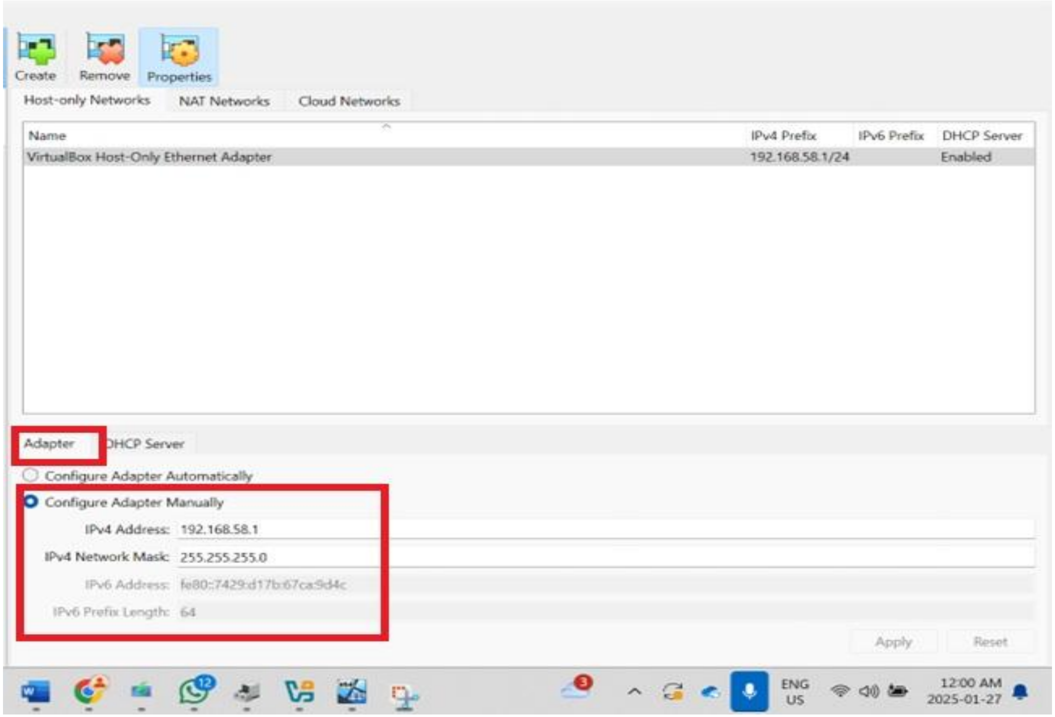
MAC Address: 080027ED7881

☑ Cable Connected

Serial Ports — Port 1

□ Enable Serial Port

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



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.58.1/24		Enabled

Adapter | DHCP Server

○ Configure Adapter Automatically

● Configure Adapter Manually

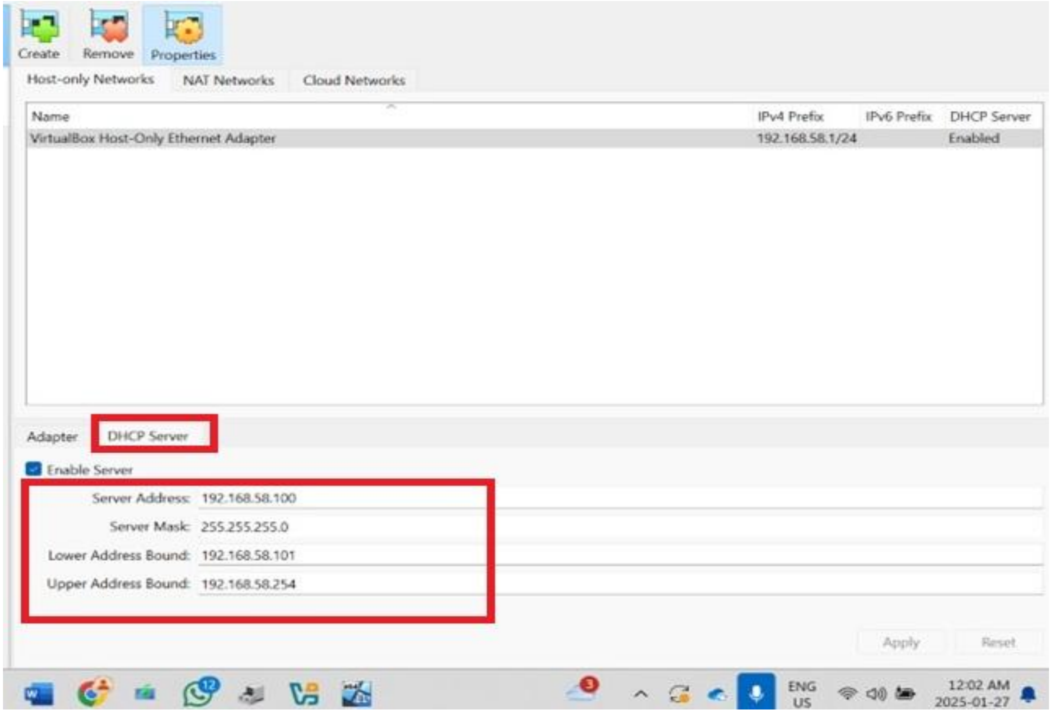
IPv4 Address: 192.168.58.1

IPv4 Network Mask: 255.255.255.0

IPv6 Address: fe80::7429:d17b:67ca:9d4c

IPv6 Prefix Length: 64

- **Set up DHCP Server to .58**



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
VirtualBox Host-Only Ethernet Adapter	192.168.58.1/24		Enabled

Adapter | DHCP Server

☑ Enable Server

Server Address: 192.168.58.100

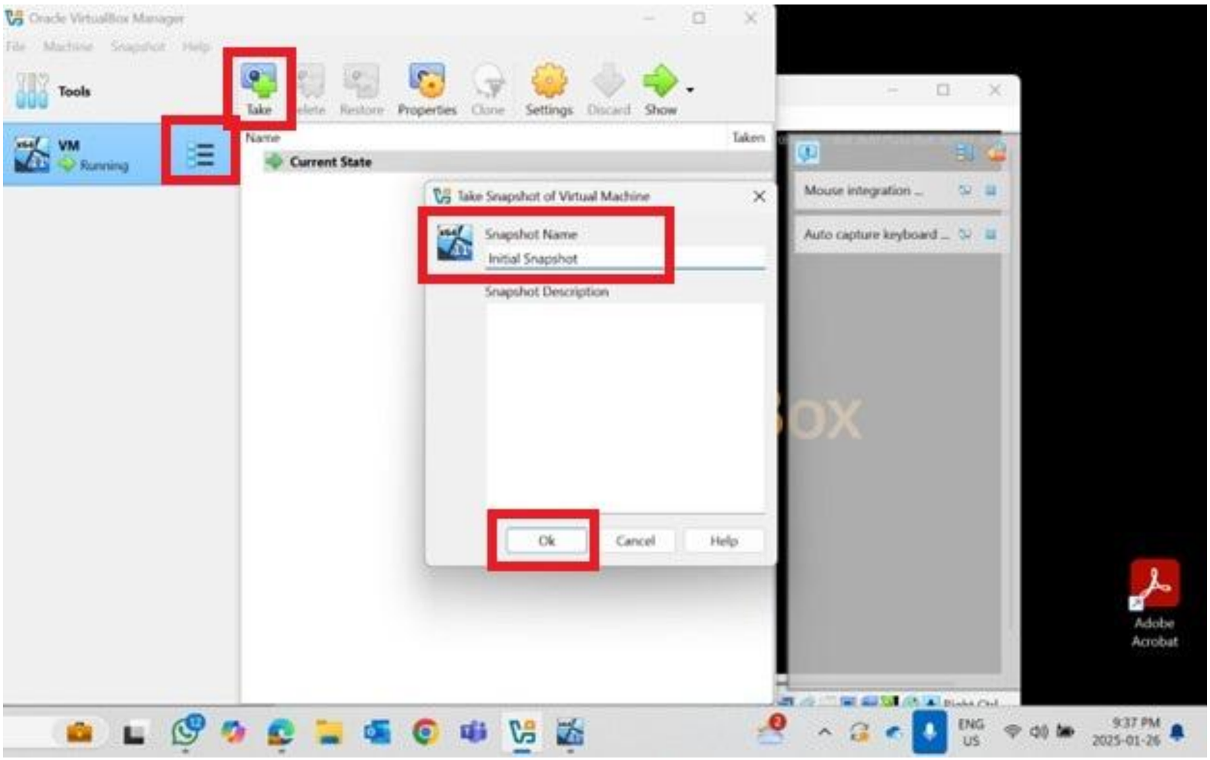
Server Mask: 255.255.255.0

Lower Address Bound: 192.168.58.101

Upper Address Bound: 192.168.58.254

2. **Take a Snapshot:**

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

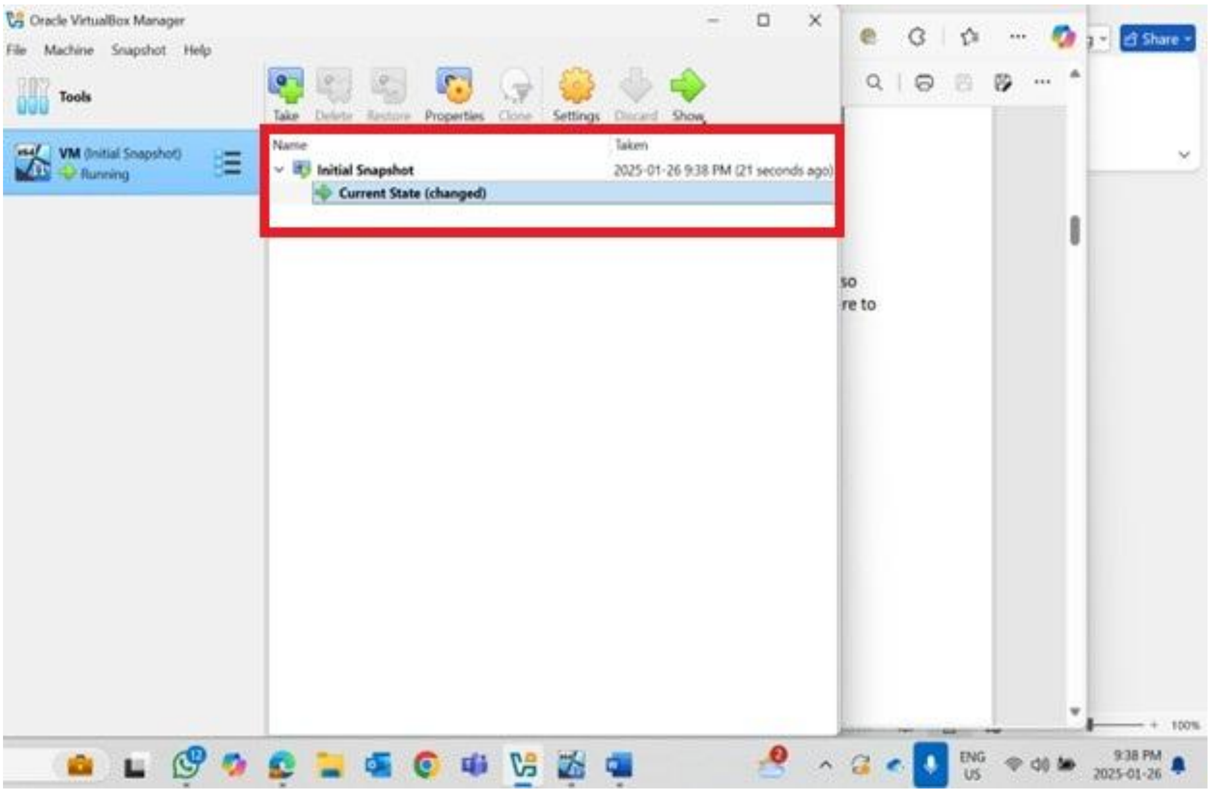


Take Snapshot of Virtual Machine

Snapshot Name: Initial Snapshot

Snapshot Description:

9:37 PM 2025-01-26



Name	Taken
Initial Snapshot	2025-01-26 9:38 PM (21 seconds ago)
Current State (changed)	

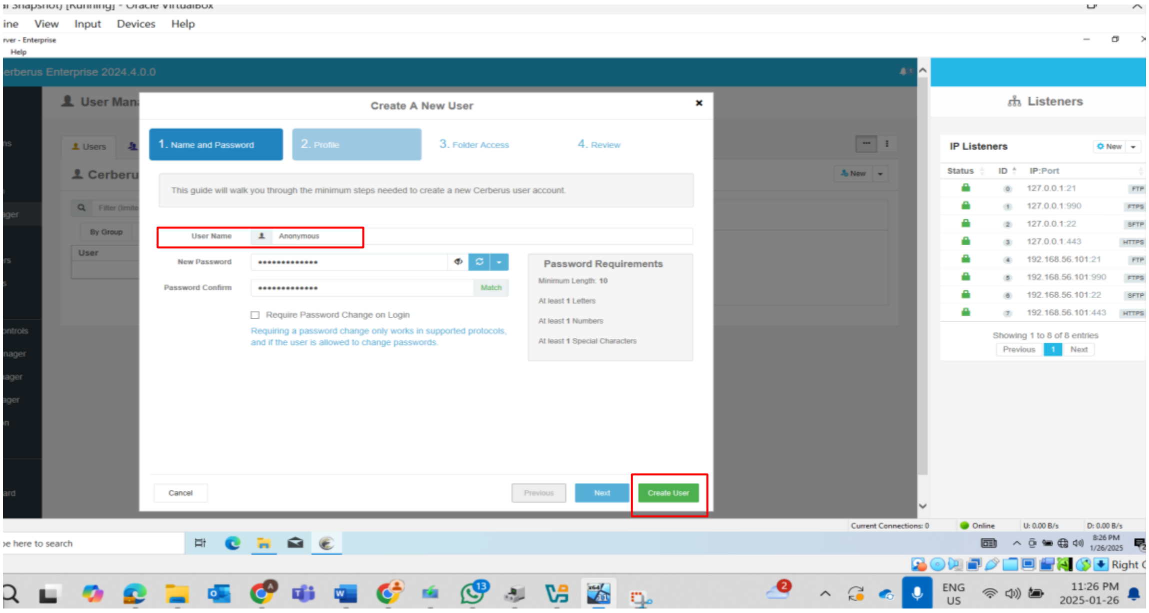
9:38 PM 2025-01-26

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**.



Create A New User

1. Name and Password · 2. Profile · 3. Folder Access · 4. Review

This guide will walk you through the minimum steps needed to create a new Cerberus user account.

User Name: Anonymous

New Password: ••••••••••••••

Password Confirm: •••••••••••••• Match

□ Require Password Change on Login

Requiring a password change only works in supported protocols, and if the user is allowed to change passwords.

Password Requirements

Minimum Length: 10

At least 1 Letters

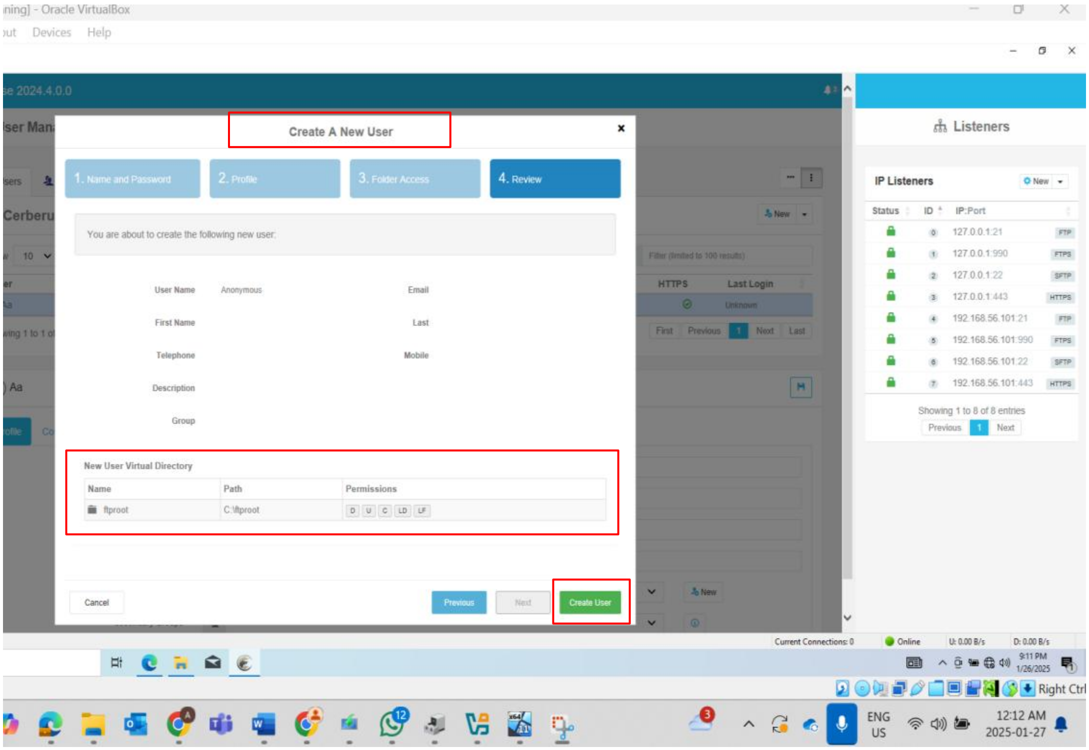
At least 1 Numbers

At least 1 Special Characters

IP Listeners

Status	ID	IP:Port	
🔒	0	127.0.0.1:21	FTP
🔒	1	127.0.0.1:990	FTPS
🔒	2	127.0.0.1:22	SFTP
🔒	3	127.0.0.1:443	HTTPS
🔒	4	192.168.56.101:21	FTP
🔒	5	192.168.56.101:990	FTPS
🔒	6	192.168.56.101:22	SFTP
🔒	7	192.168.56.101:443	HTTPS

Showing 1 to 8 of 8 entries



Create A New User

1. Name and Password · 2. Profile · 3. Folder Access · 4. Review

You are about to create the following new user:

User Name: Anonymous

First Name:

Telephone:

Description:

Group:

Email:

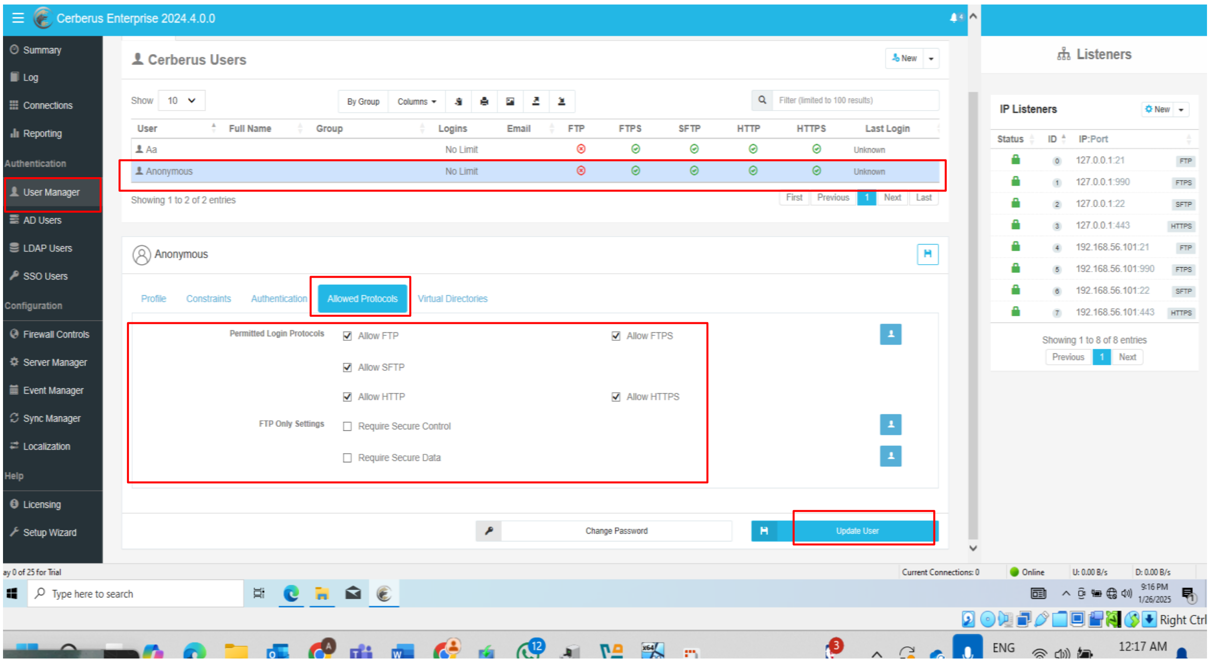
Last:

Mobile:

New User Virtual Directory

Name	Path	Permissions
ftproot	C:\ftproot	D U C LD LF

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



Cerberus Users

Show 10

User	Full Name	Group	Logins	Email	FTP	FTPS	SFTP	HTTP	HTTPS	Last Login
Aa			No Limit		⊗	✓	✓	✓	✓	Unknown
Anonymous			No Limit		⊗	✓	✓	✓	✓	Unknown

Showing 1 to 2 of 2 entries

Anonymous

Profile | Constraints | Authentication | Allowed Protocols | Virtual Directories

Permitted Login Protocols: ☑ Allow FTP ☑ Allow FTPS ☑ Allow SFTP ☑ Allow HTTP ☑ Allow HTTPS

FTP Only Settings: ☐ Require Secure Control ☐ Require Secure Data

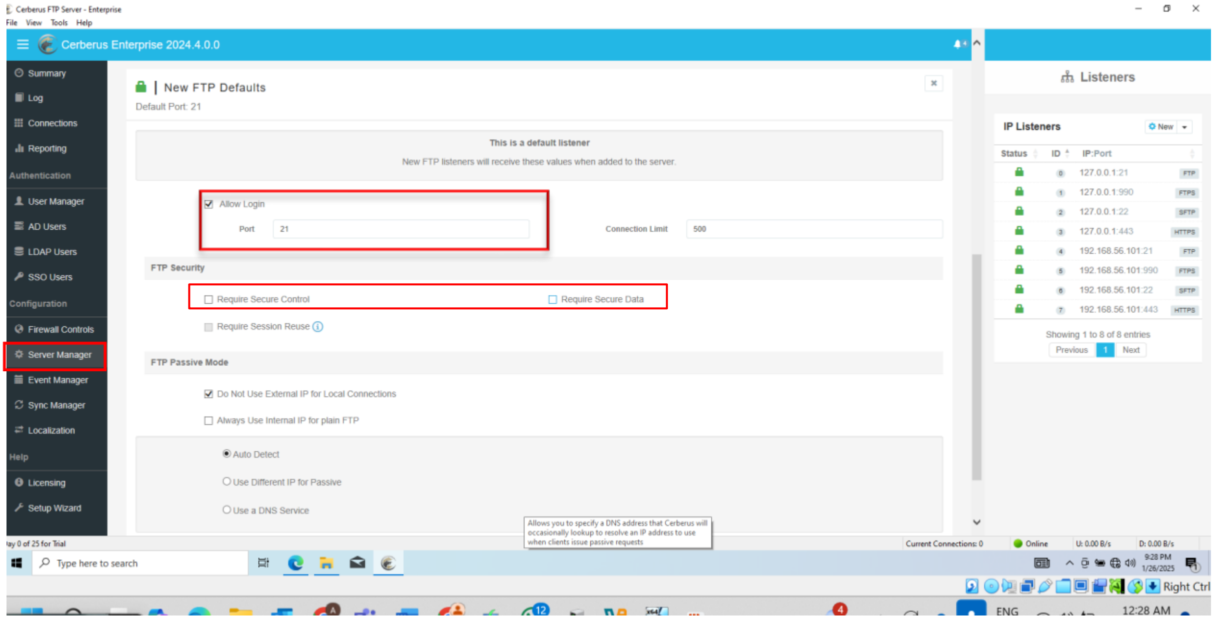
IP Listeners

Status	ID	IP:Port	
	0	127.0.0.1:21	FTP
	1	127.0.0.1:990	FTPS
	2	127.0.0.1:22	SFTP
	3	127.0.0.1:443	HTTPS
	4	192.168.56.101:21	FTP
	5	192.168.56.101:990	FTPS
	6	192.168.56.101:22	SFTP
	7	192.168.56.101:443	HTTPS

Showing 1 to 8 of 8 entries

ay 0 of 25 for Trial

- Disable secure control and data



New FTP Defaults

Default Port: 21

This is a default listener

New FTP listeners will receive these values when added to the server.

☑ Allow Login

Port: 21 Connection Limit: 500

FTP Security

☐ Require Secure Control ☐ Require Secure Data

☐ Require Session Reuse

FTP Passive Mode

☑ Do Not Use External IP for Local Connections

☐ Always Use Internal IP for plain FTP

● Auto Detect

○ Use Different IP for Passive

○ Use a DNS Service

Allows you to specify a DNS address that Cerberus will occasionally lookup to resolve an IP address to use when clients issue passive requests

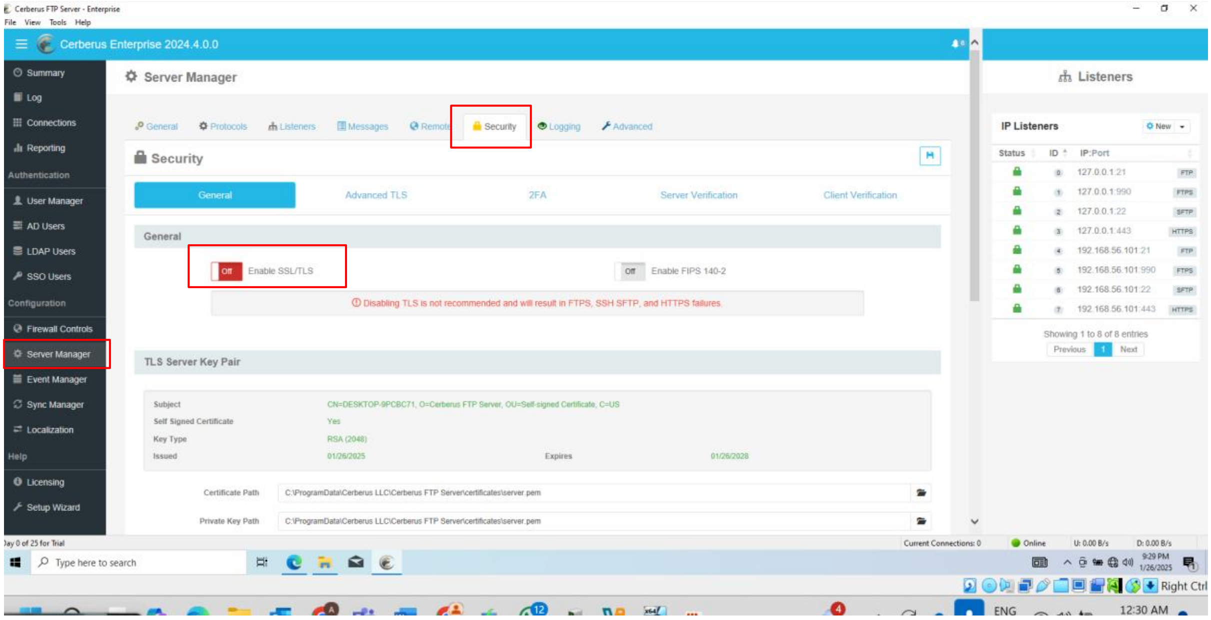
IP Listeners

Status	ID	IP:Port	
	0	127.0.0.1:21	FTP
	1	127.0.0.1:990	FTPS
	2	127.0.0.1:22	SFTP
	3	127.0.0.1:443	HTTPS
	4	192.168.56.101:21	FTP
	5	192.168.56.101:990	FTPS
	6	192.168.56.101:22	SFTP
	7	192.168.56.101:443	HTTPS

Showing 1 to 8 of 8 entries

ay 0 of 25 for Trial

- Disable SSL/TLS



Server Manager

Security

General

Off Enable SSL/TLS

Off Enable FIPS 140-2

Disabling TLS is not recommended and will result in FTPS, SSH SFTP, and HTTPS failures.

TLS Server Key Pair

Subject	CN=DESKTOP-9PCBC71, 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

Private Key Path: C:\ProgramData\Cerberus LLC\Cerberus FTP Server\certificates\server.pem

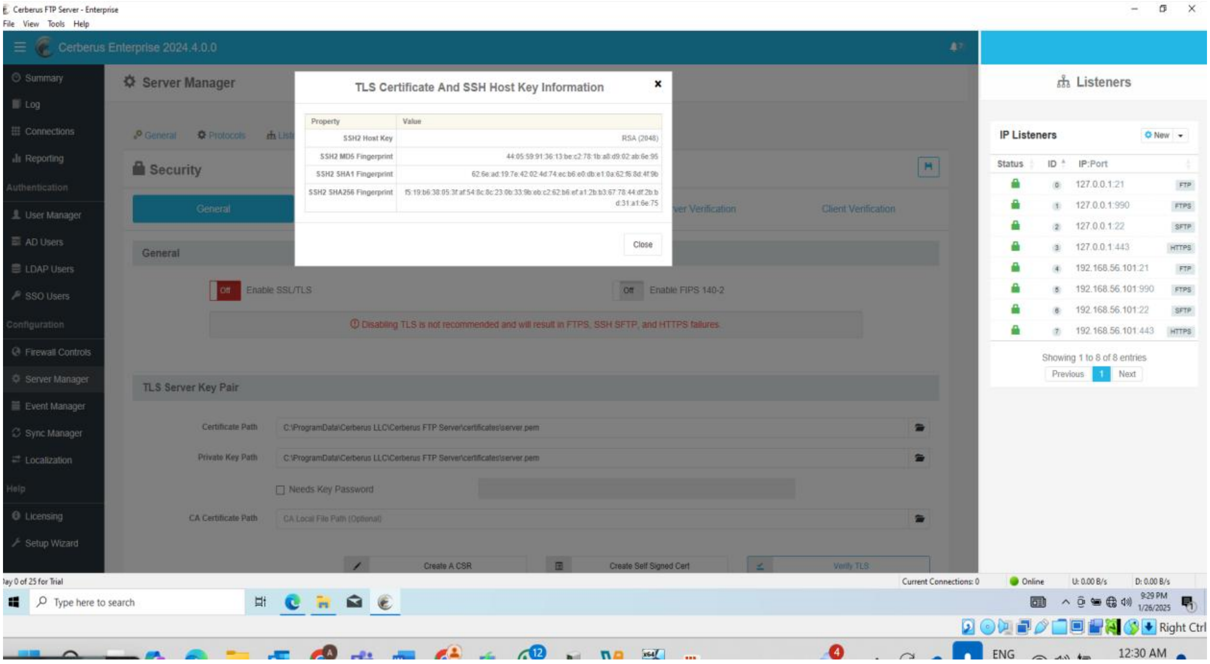
IP Listeners

Status	ID	IP:Port	
🔒	0	127.0.0.1:21	FTP
🔒	1	127.0.0.1:990	FTPS
🔒	2	127.0.0.1:22	SFTP
🔒	3	127.0.0.1:443	HTTPS
🔒	4	192.168.56.101:21	FTP
🔒	5	192.168.56.101:990	FTPS
🔒	6	192.168.56.101:22	SFTP
🔒	7	192.168.56.101:443	HTTPS

Showing 1 to 8 of 8 entries

Day 0 of 25 for Trial | Current Connections: 0 | Online | U: 0.00 B/s | D: 0.00 B/s

9:29 PM 1/26/2025



TLS Certificate And SSH Host Key Information

Property	Value
SSH2 Host Key	RSA (2048)
SSH2 MD5 Fingerprint	44:05:59:91:36:13:be:c2:78:1b:a8:d9:02:ab:6e:95
SSH2 SHA1 Fingerprint	62:6e:ad:19:7e:42:02:4d:74:ec:b6:e0:db:e1:0a:62:f6:8d:4f:9b
SSH2 SHA256 Fingerprint	f5:19:b6:38:05:3f:af:54:8c:8c:23:0b:33:9b:eb:c2:62:b6:ef:a1:2b:b3:67:78:44:df:2b:bd:31:a1:6e:75

Off Enable SSL/TLS

Off Enable FIPS 140-2

Disabling TLS is not recommended and will result in FTPS, SSH SFTP, and HTTPS failures.

TLS Server Key Pair

Certificate Path: C:\ProgramData\Cerberus LLC\Cerberus FTP Server\certificates\server.pem

Private Key Path: C:\ProgramData\Cerberus LLC\Cerberus FTP Server\certificates\server.pem

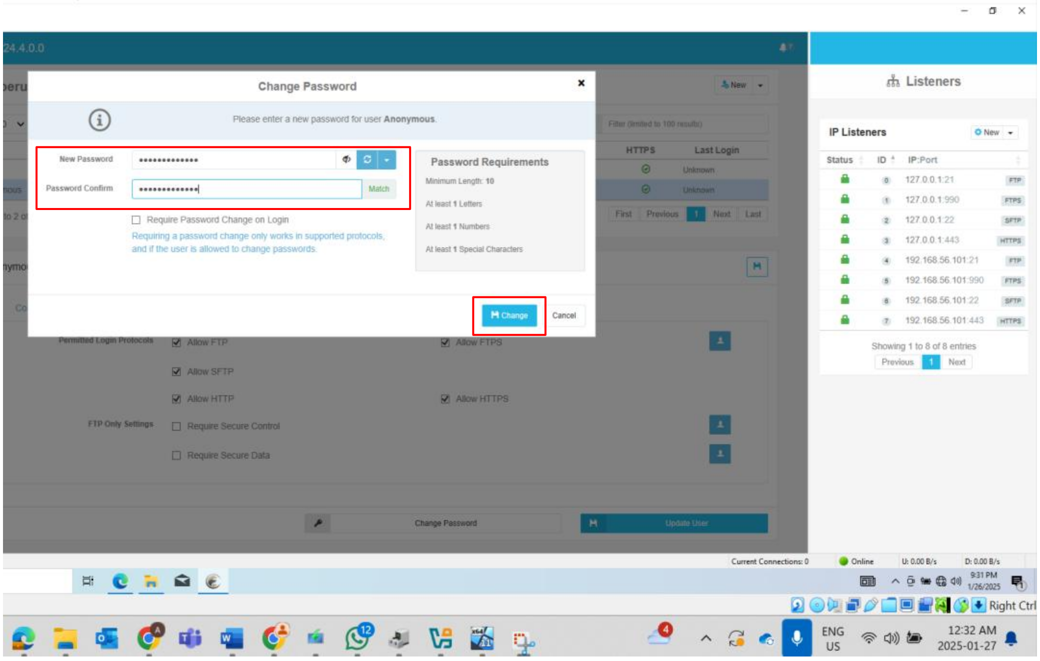
□ Needs Key Password

CA Certificate Path: CA Local File Path (Optional)

Day 0 of 25 for Trial | Current Connections: 0 | Online | U: 0.00 B/s | D: 0.00 B/s

9:29 PM 1/26/2025

- **Setting password for Anonymous user:**



Change Password

Please enter a new password for user **Anonymous**.

New Password: ••••••••••••••

Password Confirm: •••••••••••••• Match

☐ Require Password Change on Login

Requiring a password change only works in supported protocols, and if the user is allowed to change passwords.

Password Requirements

Minimum Length: 10

At least 1 Letters

At least 1 Numbers

At least 1 Special Characters

Permitted Login Protocols: ☑ Allow FTP ☑ Allow FTPS ☑ Allow SFTP ☑ Allow HTTP ☑ Allow HTTPS

FTP Only Settings: ☐ Require Secure Control ☐ Require Secure Data

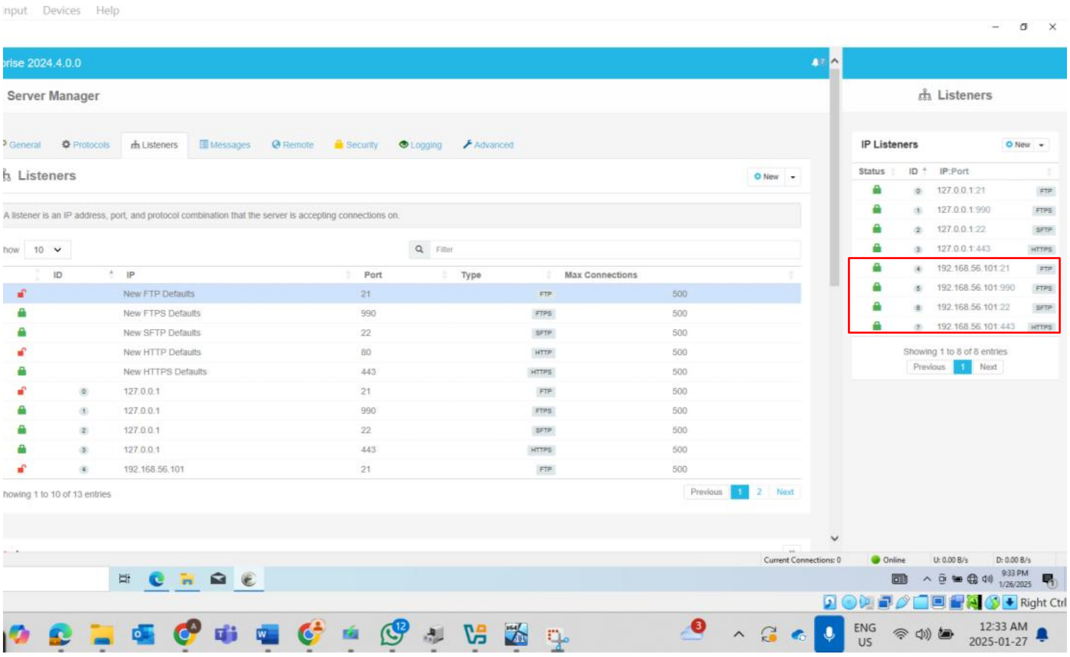
IP Listeners

Status	ID	IP:Port	
🔒	0	127.0.0.1:21	FTP
🔒	1	127.0.0.1:990	FTPS
🔒	2	127.0.0.1:22	SFTP
🔒	3	127.0.0.1:443	HTTPS
🔒	4	192.168.56.101:21	FTP
🔒	5	192.168.56.101:990	FTPS
🔒	6	192.168.56.101:22	SFTP
🔒	7	192.168.56.101:443	HTTPS

Showing 1 to 8 of 8 entries

Current Connections: 0 Online U: 0.00 B/s D: 0.00 B/s

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



Server Manager

General Protocols Listeners Messages Remote Security Logging Advanced

Listeners

A listener is an IP address, port, and protocol combination that the server is accepting connections on.

	ID	IP	Port	Type	Max Connections
🔓		New FTP Defaults	21	FTP	500
🔒		New FTPS Defaults	990	FTPS	500
🔒		New SFTP Defaults	22	SFTP	500
🔓		New HTTP Defaults	80	HTTP	500
🔒		New HTTPS Defaults	443	HTTPS	500
🔓	0	127.0.0.1	21	FTP	500
🔒	1	127.0.0.1	990	FTPS	500
🔒	2	127.0.0.1	22	SFTP	500
🔒	3	127.0.0.1	443	HTTPS	500
🔓	4	192.168.56.101	21	FTP	500

howing 1 to 10 of 13 entries

IP Listeners

Status	ID	IP:Port	
🔒	0	127.0.0.1:21	FTP
🔒	1	127.0.0.1:990	FTPS
🔒	2	127.0.0.1:22	SFTP
🔒	3	127.0.0.1:443	HTTPS
🔒	4	192.168.56.101:21	FTP
🔒	5	192.168.56.101:990	FTPS
🔒	6	192.168.56.101:22	SFTP
🔒	7	192.168.56.101:443	HTTPS

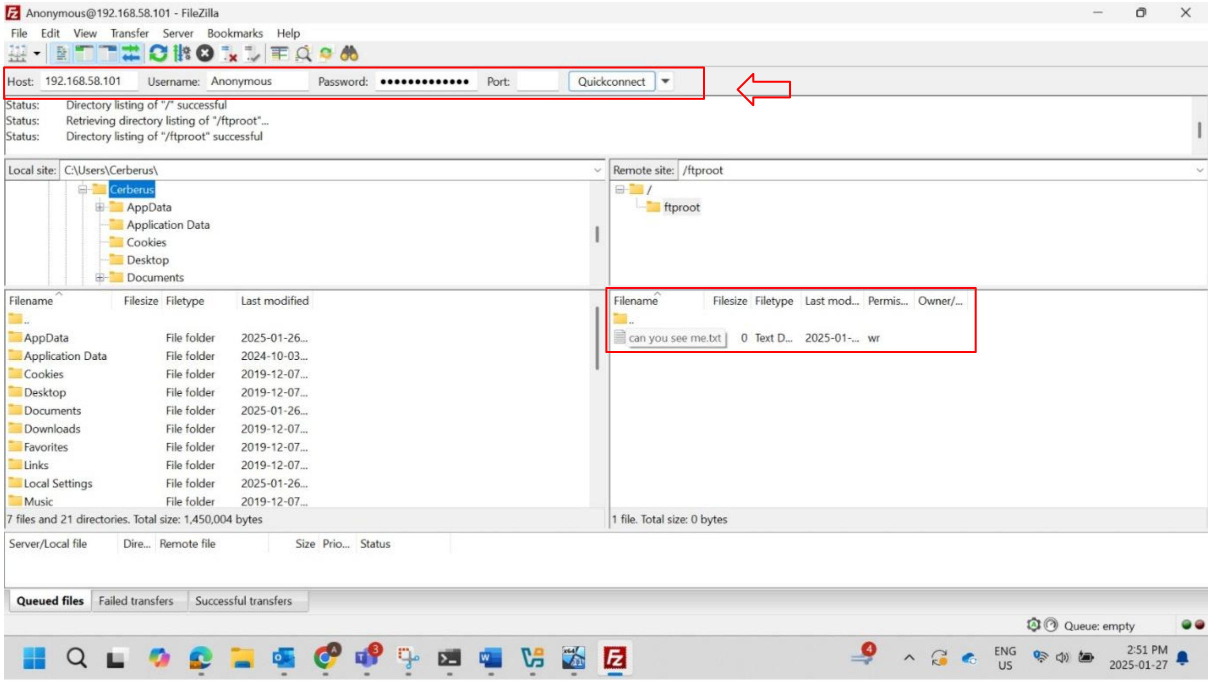
Showing 1 to 8 of 8 entries

Current Connections: 0 Online U: 0.00 B/s D: 0.00 B/s

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**:


Anonymous@192.168.58.101 - FileZilla

Host: 192.168.58.101 Username: Anonymous Password: ••••••••••••• Port:

```
Status:     Directory listing of "/" successful
Status:     Retrieving directory listing of "/ftproot"...
Status:     Directory listing of "/ftproot" successful
```

Local site: C:\Users\Cerberus\

Filename	Filesize	Filetype	Last modified
..			
AppData		File folder	2025-01-26...
Application Data		File folder	2024-10-03...
Cookies		File folder	2019-12-07...
Desktop		File folder	2019-12-07...
Documents		File folder	2025-01-26...
Downloads		File folder	2019-12-07...
Favorites		File folder	2019-12-07...
Links		File folder	2019-12-07...
Local Settings		File folder	2025-01-26...
Music		File folder	2019-12-07...

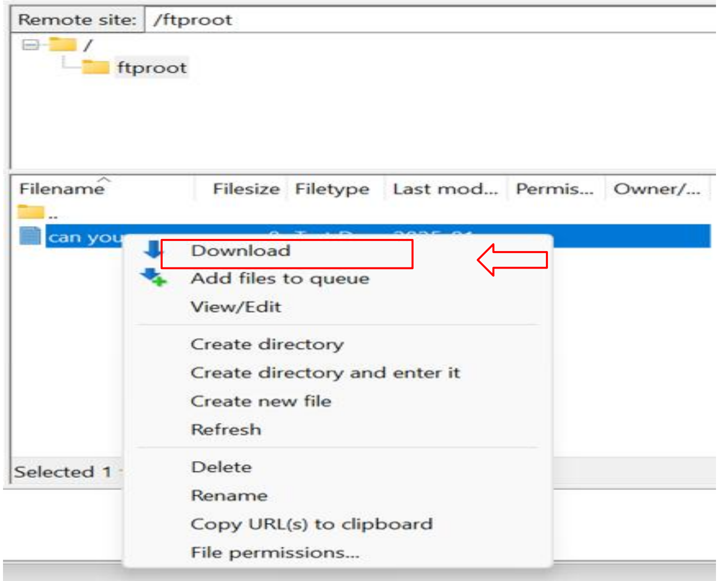
7 files and 21 directories. Total size: 1,450,004 bytes

Remote site: /ftproot

Filename	Filesize	Filetype	Last mod...	Permis...	Owner/...
..					
can you see me.txt	0	Text D...	2025-01-...	wr	

1 file. Total size: 0 bytes

Queue: empty


Remote site: /ftproot

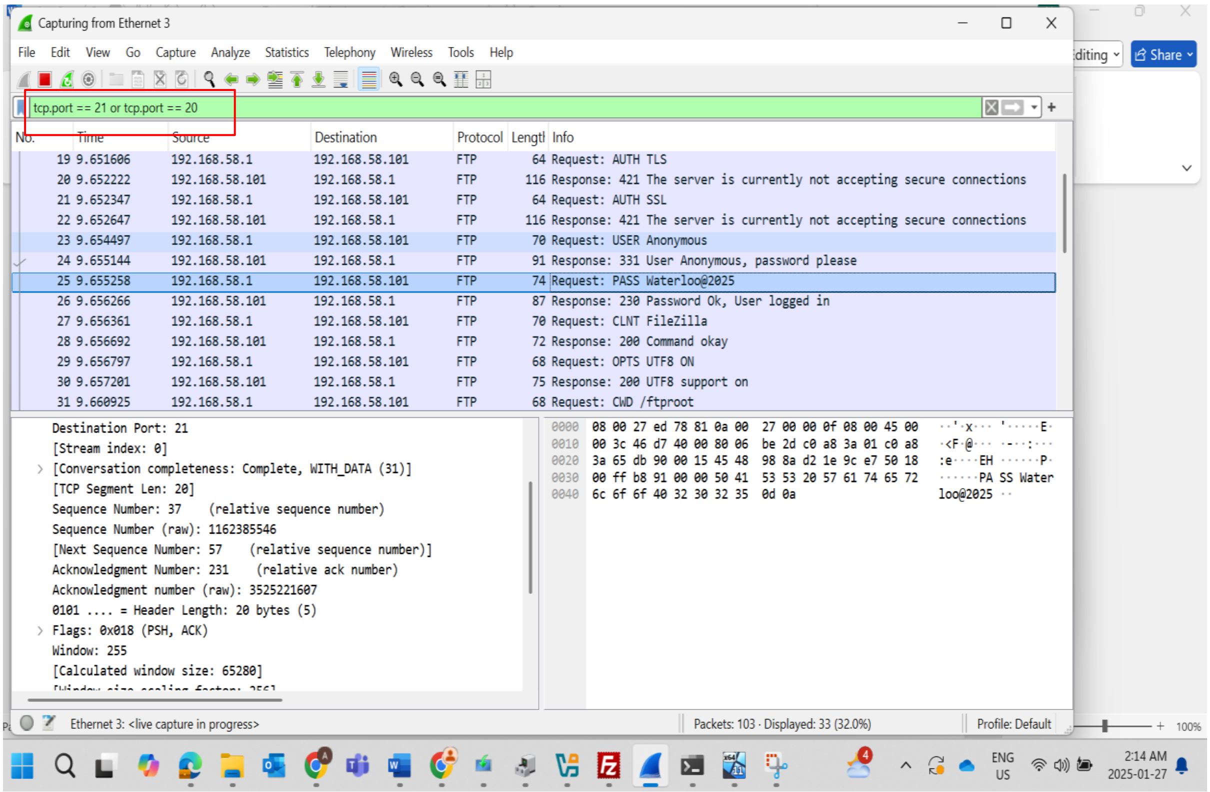
Filename	Filesize	Filetype	Last mod...	Permis...	Owner/...
..					
can you					

Selected 1

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


Capturing from Ethernet 3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
diting
Share

```
tcp.port == 21 or tcp.port == 20
```

```
No.  Time      Source          Destination     Protocol Lengtl Info
  19 9.651606  192.168.58.1    192.168.58.101  FTP       64 Request: AUTH TLS
  20 9.652222  192.168.58.101  192.168.58.1    FTP      116 Response: 421 The server is currently not accepting secure connections
  21 9.652347  192.168.58.1    192.168.58.101  FTP       64 Request: AUTH SSL
  22 9.652647  192.168.58.101  192.168.58.1    FTP      116 Response: 421 The server is currently not accepting secure connections
  23 9.654497  192.168.58.1    192.168.58.101  FTP       70 Request: USER Anonymous
  24 9.655144  192.168.58.101  192.168.58.1    FTP       91 Response: 331 User Anonymous, password please
  25 9.655258  192.168.58.1    192.168.58.101  FTP       74 Request: PASS Waterloo@2025
  26 9.656266  192.168.58.101  192.168.58.1    FTP       87 Response: 230 Password Ok, User logged in
  27 9.656361  192.168.58.1    192.168.58.101  FTP       70 Request: CLNT FileZilla
  28 9.656692  192.168.58.101  192.168.58.1    FTP       72 Response: 200 Command okay
  29 9.656797  192.168.58.1    192.168.58.101  FTP       68 Request: OPTS UTF8 ON
  30 9.657201  192.168.58.101  192.168.58.1    FTP       75 Response: 200 UTF8 support on
  31 9.660925  192.168.58.1    192.168.58.101  FTP       68 Request: CWD /ftproot
```

```
    Destination Port: 21
    [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 20]
    Sequence Number: 37    (relative sequence number)
    Sequence Number (raw): 1162385546
    [Next Sequence Number: 57    (relative sequence number)]
    Acknowledgment Number: 231    (relative ack number)
    Acknowledgment number (raw): 3525221607
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 255
    [Calculated window size: 65280]
```

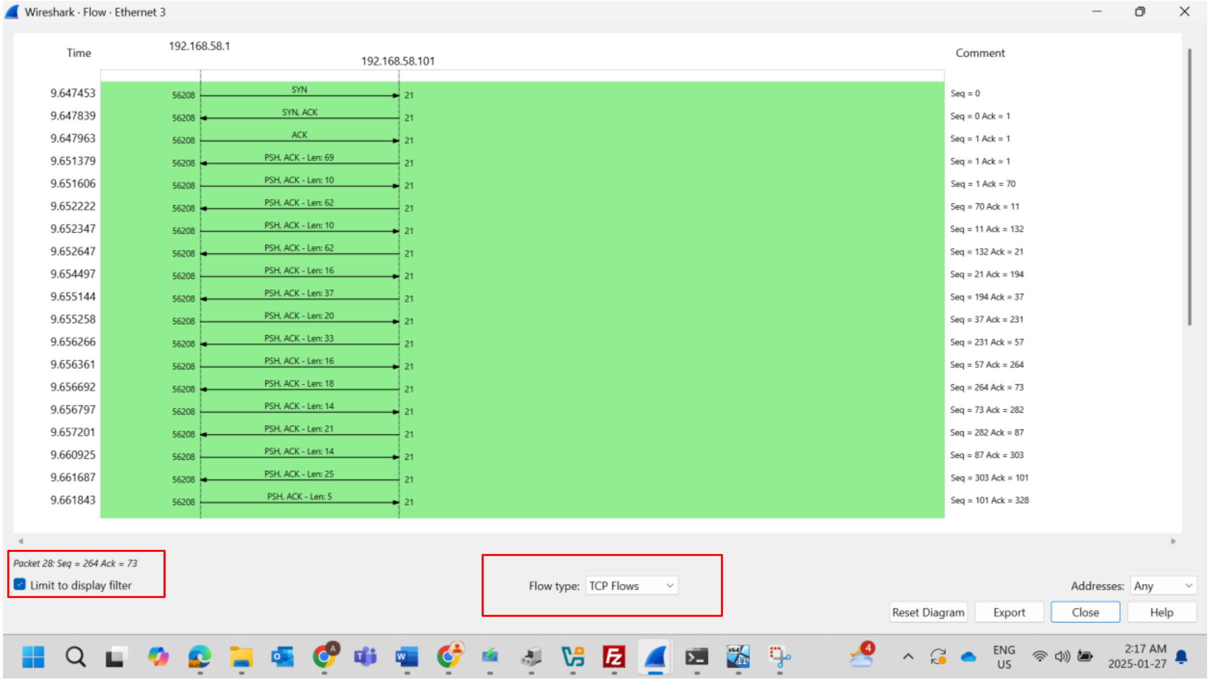
```
0000  08 00 27 ed 78 81 0a 00  27 00 00 0f 08 00 45 00   ··'·x··· '·····E·
0010  00 3c 46 d7 40 00 80 06  be 2d c0 a8 3a 01 c0 a8   ·<F·@··· ·-··:···
0020  3a 65 db 90 00 15 45 48  98 8a d2 1e 9c e7 50 18   :e····EH ······P·
0030  00 ff b8 91 00 00 50 41  53 53 20 57 61 74 65 72   ······PA SS Water
0040  6c 6f 6f 40 32 30 32 35  0d 0a                     loo@2025 ··
```

Ethernet 3: <live capture in progress>

Packets: 103 · Displayed: 33 (32.0%)

Profile: Default

Output #2: Flow graph in Wireshark



```
Time        192.168.58.1   192.168.58.101                 Comment
9.647453    56208 --SYN-->                        21      Seq = 0
9.647839    56208 <--SYN, ACK--                   21      Seq = 0 Ack = 1
9.647963    56208 --ACK-->                        21      Seq = 1 Ack = 1
9.651379    56208 <--PSH, ACK - Len: 69--         21      Seq = 1 Ack = 1
9.651606    56208 --PSH, ACK - Len: 10-->         21      Seq = 1 Ack = 70
9.652222    56208 <--PSH, ACK - Len: 62--         21      Seq = 70 Ack = 11
9.652347    56208 --PSH, ACK - Len: 10-->         21      Seq = 11 Ack = 132
9.652647    56208 <--PSH, ACK - Len: 62--         21      Seq = 132 Ack = 21
9.654497    56208 --PSH, ACK - Len: 16-->         21      Seq = 21 Ack = 194
9.655144    56208 <--PSH, ACK - Len: 37--         21      Seq = 194 Ack = 37
9.655258    56208 --PSH, ACK - Len: 20-->         21      Seq = 37 Ack = 231
9.656266    56208 <--PSH, ACK - Len: 33--         21      Seq = 231 Ack = 57
9.656361    56208 --PSH, ACK - Len: 16-->         21      Seq = 57 Ack = 264
9.656692    56208 <--PSH, ACK - Len: 18--         21      Seq = 264 Ack = 73
9.656797    56208 --PSH, ACK - Len: 14-->         21      Seq = 73 Ack = 282
9.657201    56208 <--PSH, ACK - Len: 21--         21      Seq = 282 Ack = 87
9.660925    56208 --PSH, ACK - Len: 14-->         21      Seq = 87 Ack = 303
9.661687    56208 <--PSH, ACK - Len: 25--         21      Seq = 303 Ack = 101
9.661843    56208 --PSH, ACK - Len: 5-->          21      Seq = 101 Ack = 328
```

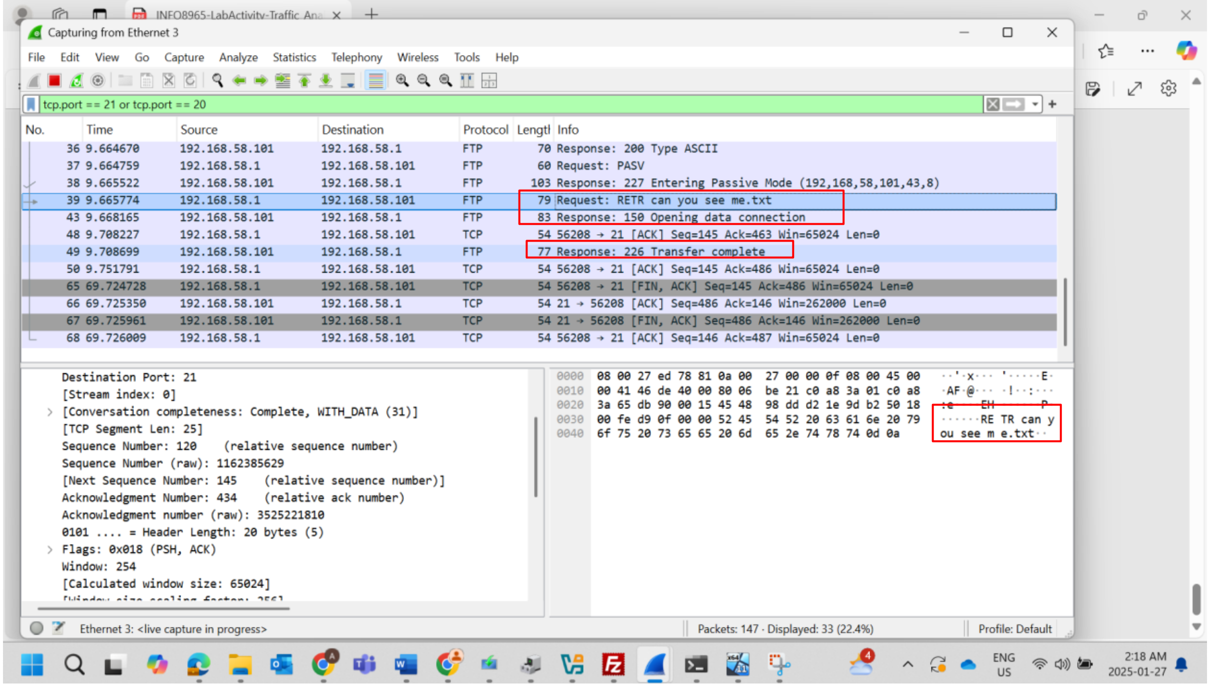
Packet 28: Seq = 264 Ack = 73

☑ Limit to display filter

Flow type: TCP Flows

Addresses: Any

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



tcp.port == 21 or tcp.port == 20

```
No.  Time       Source          Destination     Protocol Lengtl Info
  36 9.664670   192.168.58.101  192.168.58.1    FTP       70 Response: 200 Type ASCII
  37 9.664759   192.168.58.1    192.168.58.101  FTP       60 Request: PASV
  38 9.665522   192.168.58.101  192.168.58.1    FTP      103 Response: 227 Entering Passive Mode (192,168,58,101,43,8)
  39 9.665774   192.168.58.1    192.168.58.101  FTP       79 Request: RETR can you see me.txt
  43 9.668165   192.168.58.101  192.168.58.1    FTP       83 Response: 150 Opening data connection
  48 9.708227   192.168.58.1    192.168.58.101  TCP       54 56208 → 21 [ACK] Seq=145 Ack=463 Win=65024 Len=0
  49 9.708699   192.168.58.101  192.168.58.1    FTP       77 Response: 226 Transfer complete
  50 9.751791   192.168.58.1    192.168.58.101  TCP       54 56208 → 21 [ACK] Seq=145 Ack=486 Win=65024 Len=0
  65 69.724728  192.168.58.1    192.168.58.101  TCP       54 56208 → 21 [FIN, ACK] Seq=145 Ack=486 Win=65024 Len=0
  66 69.725350  192.168.58.101  192.168.58.1    TCP       54 21 → 56208 [ACK] Seq=486 Ack=146 Win=262000 Len=0
  67 69.725961  192.168.58.101  192.168.58.1    TCP       54 21 → 56208 [FIN, ACK] Seq=486 Ack=146 Win=262000 Len=0
  68 69.726009  192.168.58.1    192.168.58.101  TCP       54 56208 → 21 [ACK] Seq=146 Ack=487 Win=65024 Len=0
```

```
    Destination Port: 21
    [Stream index: 0]
  > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 25]
    Sequence Number: 120    (relative sequence number)
    Sequence Number (raw): 1162385629
    [Next Sequence Number: 145    (relative sequence number)]
    Acknowledgment Number: 434    (relative ack number)
    Acknowledgment number (raw): 3525221810
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 254
    [Calculated window size: 65024]
```

```
0000  08 00 27 ed 78 81 0a 00  27 00 00 0f 08 00 45 00   ··'·x···  '·····E·
0010  00 41 46 de 40 00 80 06  be 21 c0 a8 3a 01 c0 a8   ·AF·@···  ·!··:···
0020  3a 65 db 90 00 15 45 48  98 dd d2 1e 9d b2 50 18   :e····EH  ······P·
0030  00 fe d9 0f 00 00 52 45  54 52 20 63 61 6e 20 79   ······RE  TR can y
0040  6f 75 20 73 65 65 20 6d  65 2e 74 78 74 0d 0a      ou see m  e.txt··
```

Ethernet 3: <live capture in progress>

Packets: 147 · Displayed: 33 (22.4%)

Profile: Default