Packet Tracer – Configuring VPN Transport Mode

Addressing Table

Device	Private IP Address	Public IP Address	Subnet Mask	Site
Private_FTP server	10.44.2.254	N/A	255.255.255.0	Gotham Healthcare Branch
Public_FTP server	10.44.2.253	209.165.201.20	255.255.255.0	Gotham Healthcare Branch
Branch_Router	N/A	209.165.201.19	255.255.255.248	Gotham Healthcare Branch
Phil's computer	10.44.0.2	N/A	255.255.255.0	Metropolis Bank HQ

Objectives

Part 1: Sending Unencrypted FTP Traffic

Part 2: Configuring the VPN Client within Metropolis

Part 3: Sending Encrypted FTP Traffic

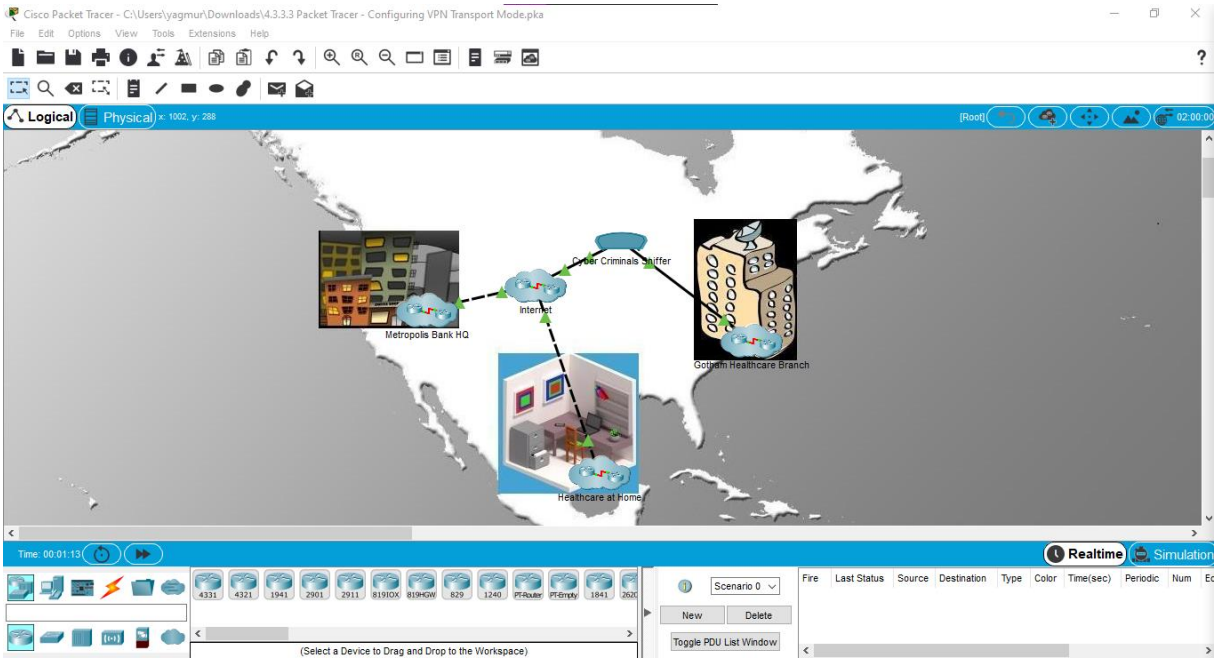
Background

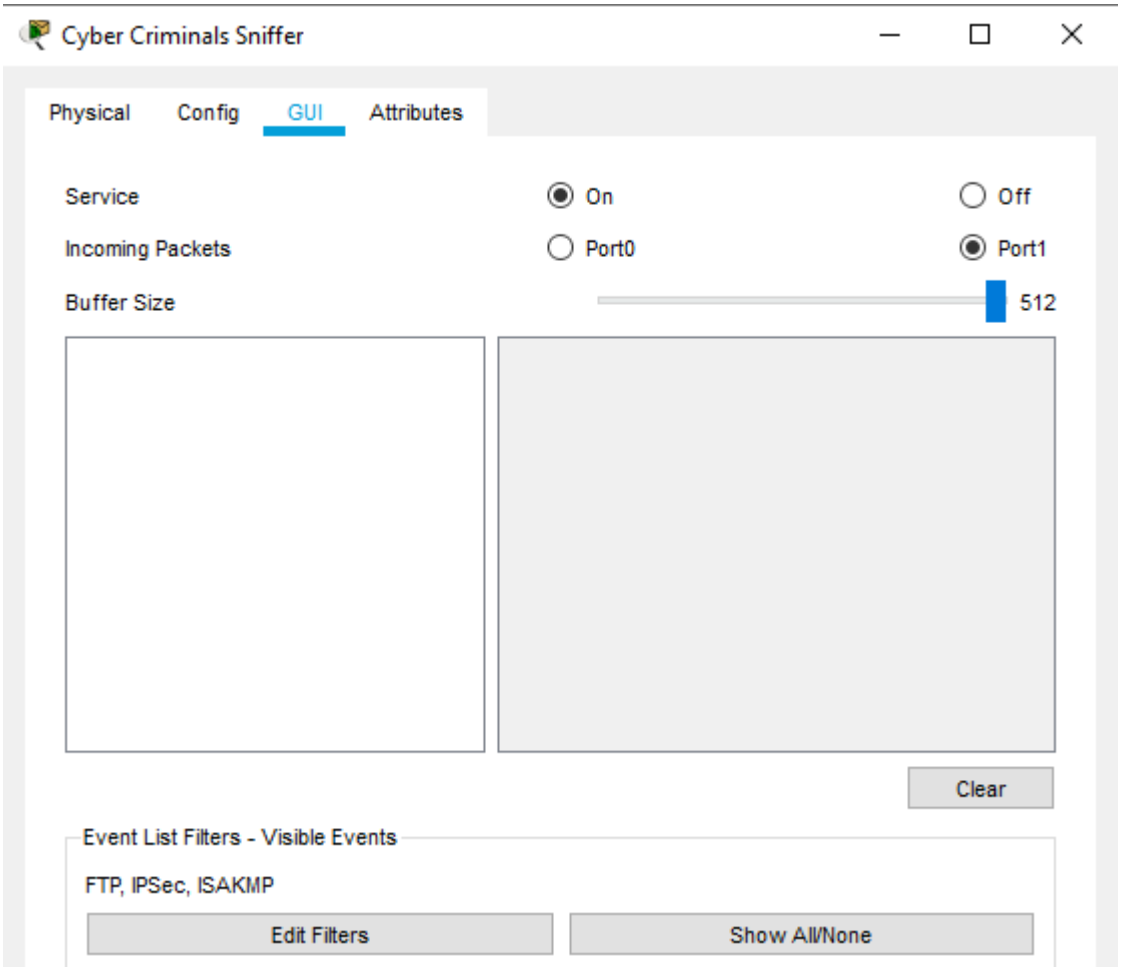
In this activity, you will observe the transfer of unencrypted FTP traffic between a client and a remote site. You will then configure a VPN client to connect to the Gotham Healthcare Branch site and send encrypted FTP traffic. The IP addressing, network configuration, and service configurations are already complete. You will use a client device within Metropolis Bank HQ to transfer unencrypted and encrypted FTP data.

Part 1: Sending Unencrypted FTP Traffic

Step 1: Access the Cyber Criminals Sniffer.

a. Click the **Cyber Criminals Sniffer** and click the **GUI** tab.



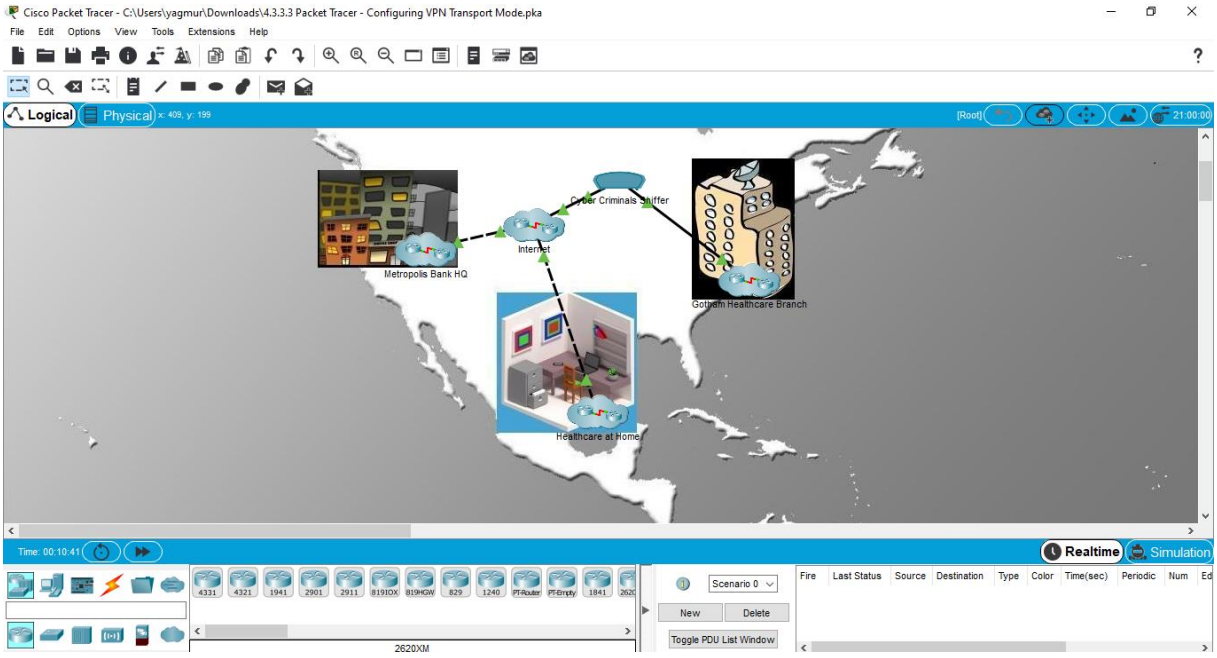


b. Click the **Clear** button to remove any possible traffic entries viewed by the sniffer.

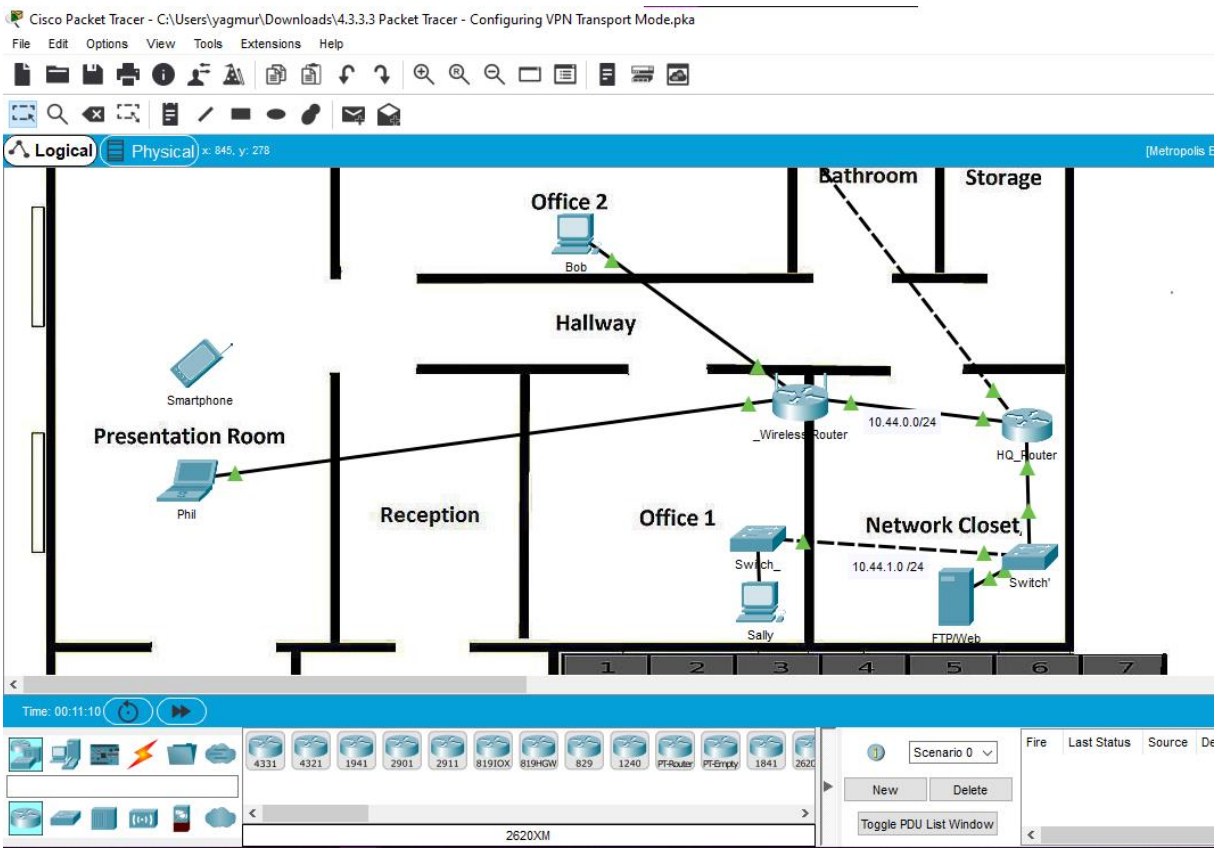
c. Minimize the **Cyber Criminals Sniffer**.

Step 2: Connect to the Public_FTP server using an insecure FTP connection.

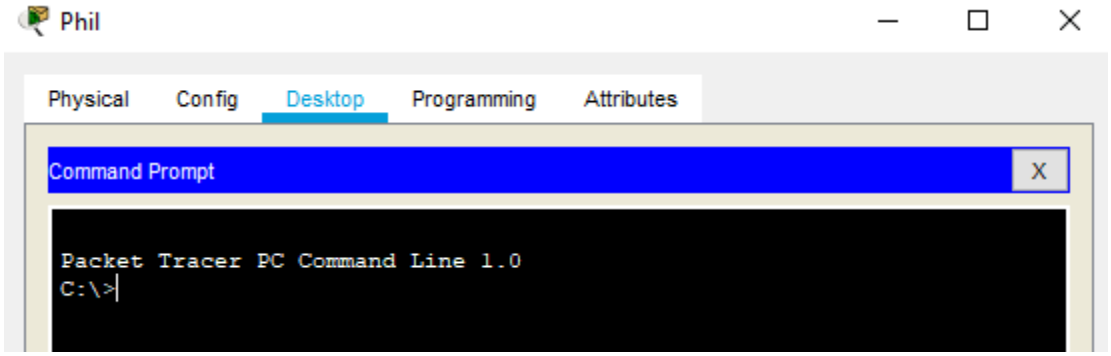
a. Click the **Metropolis Bank HQ** site and click **Phil's** laptop.

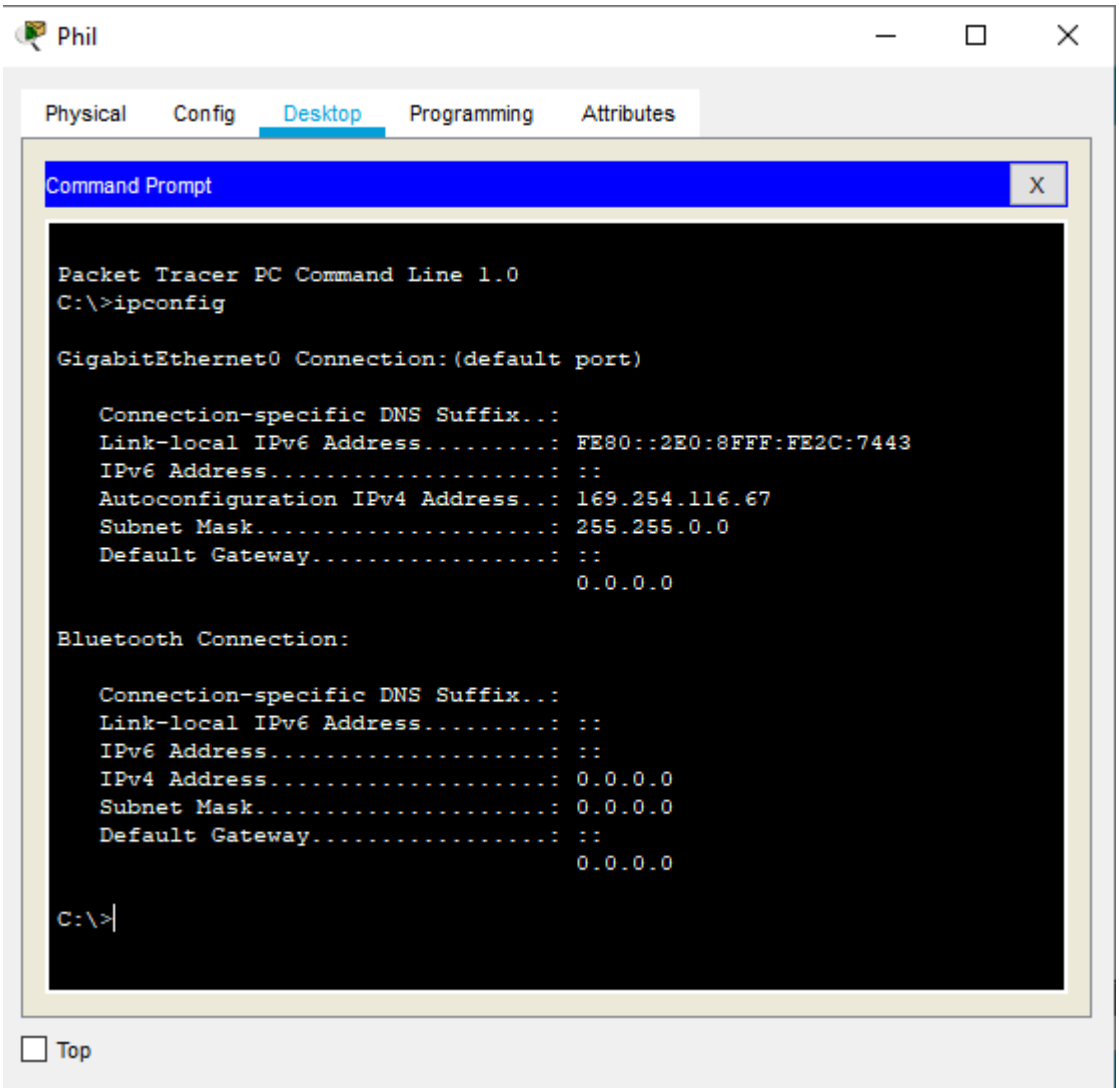


b. Click the **Desktop** tab and click on **Command Prompt**.



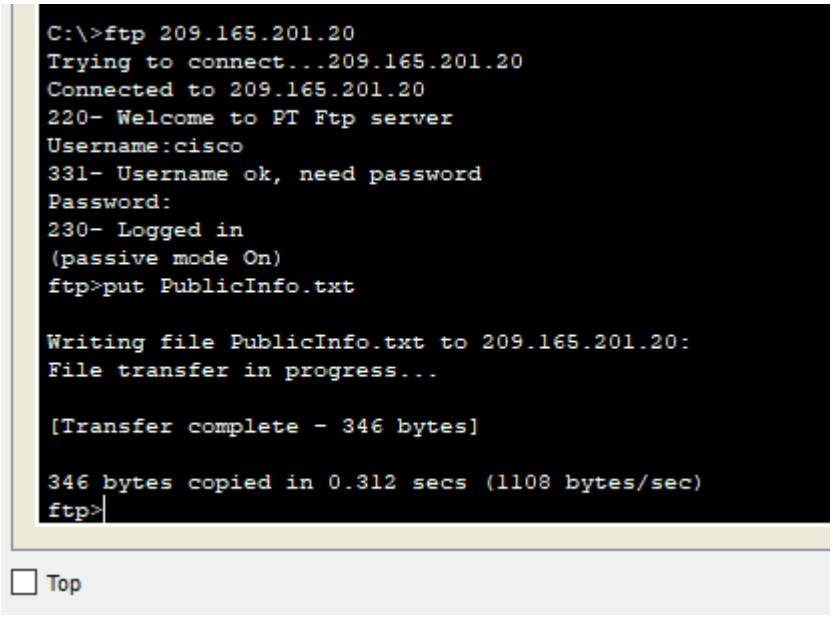
c. Use the **ipconfig** command to view the current IP address of **Phil's** computer.



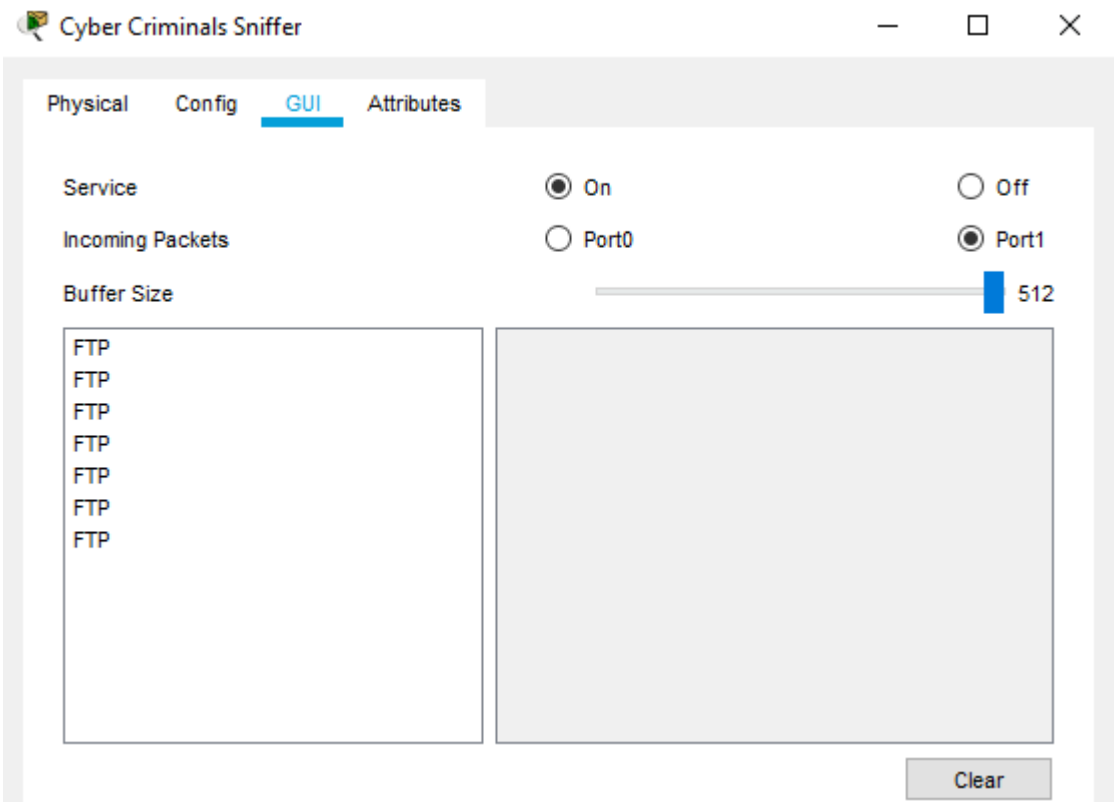


d. Connect to the **Public_FTP** server at **Gotham Healthcare Branch** by entering **ftp 209.165.201.20** in the command prompt.

e. Enter the username of **cisco** and password of **publickey** to login to the **Public_FTP** server.



f. Use the **put** command to upload the file **PublicInfo.txt** file to the **Public_FTP** server.



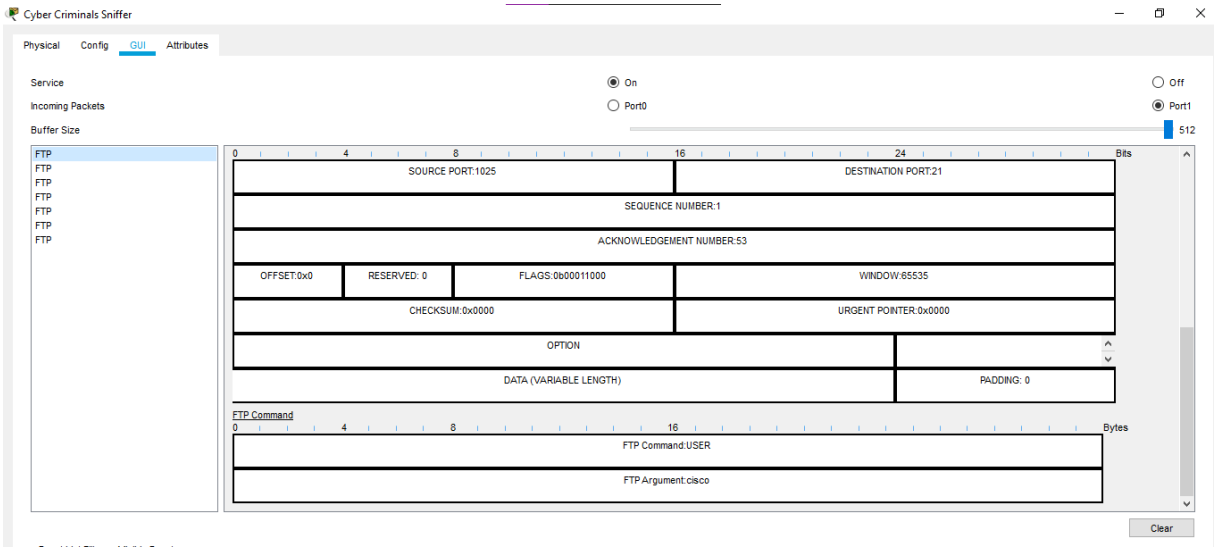
Step 3: View the traffic on the Cyber Criminals Sniffer.

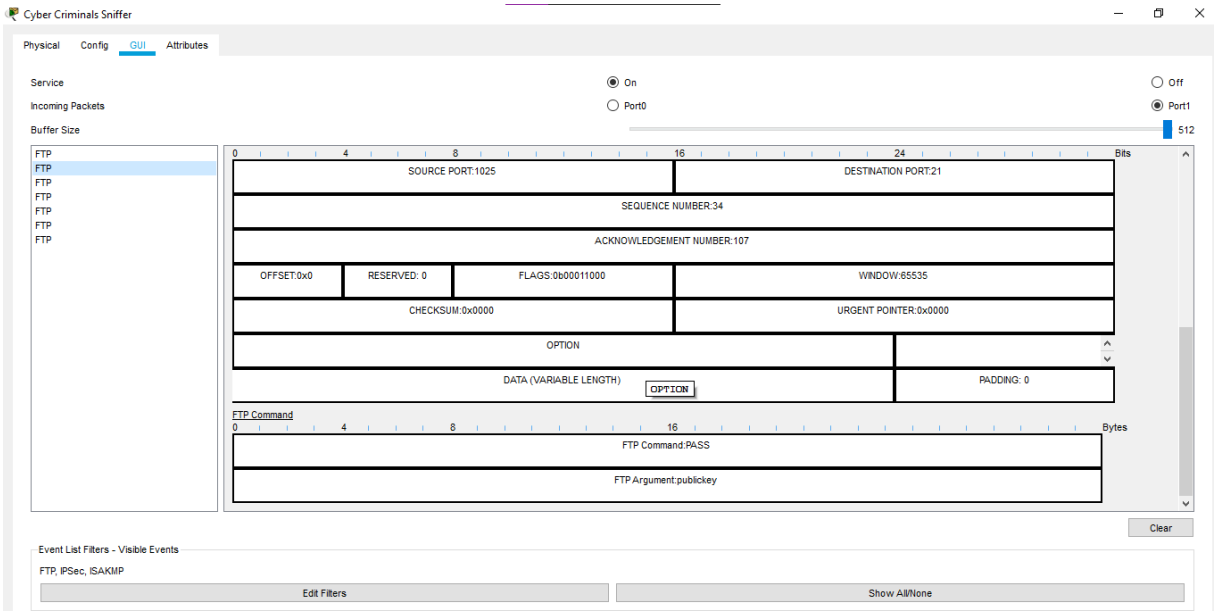
a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.

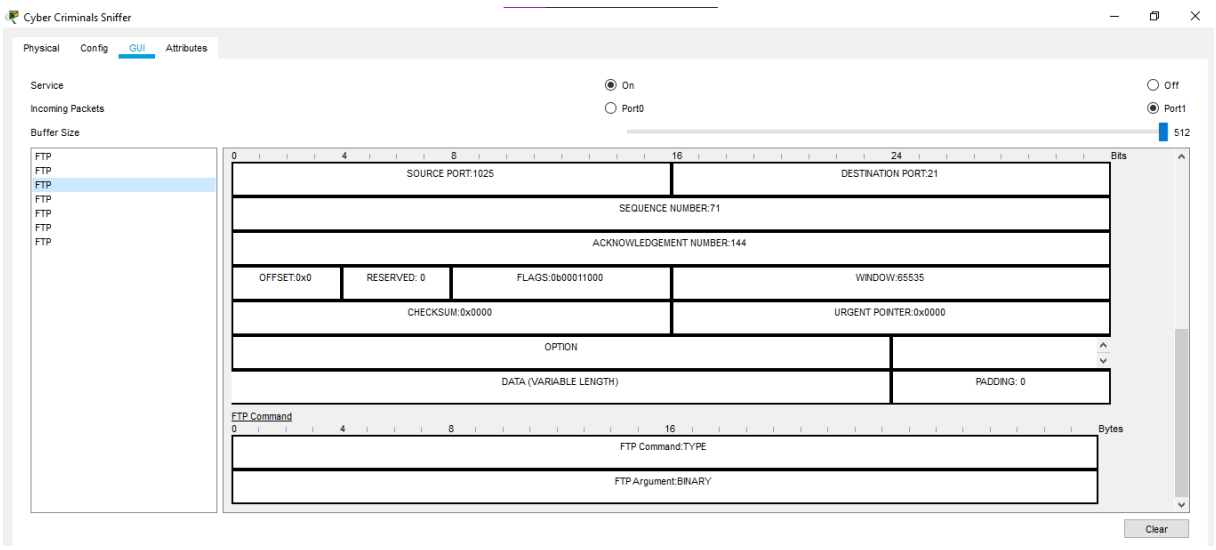
b. Click the **FTP** messages displayed on the sniffer and scroll to the bottom of each one.

What information is displayed in clear text?

USER cisco PASS publickey and the filename of PublicInfo.txt







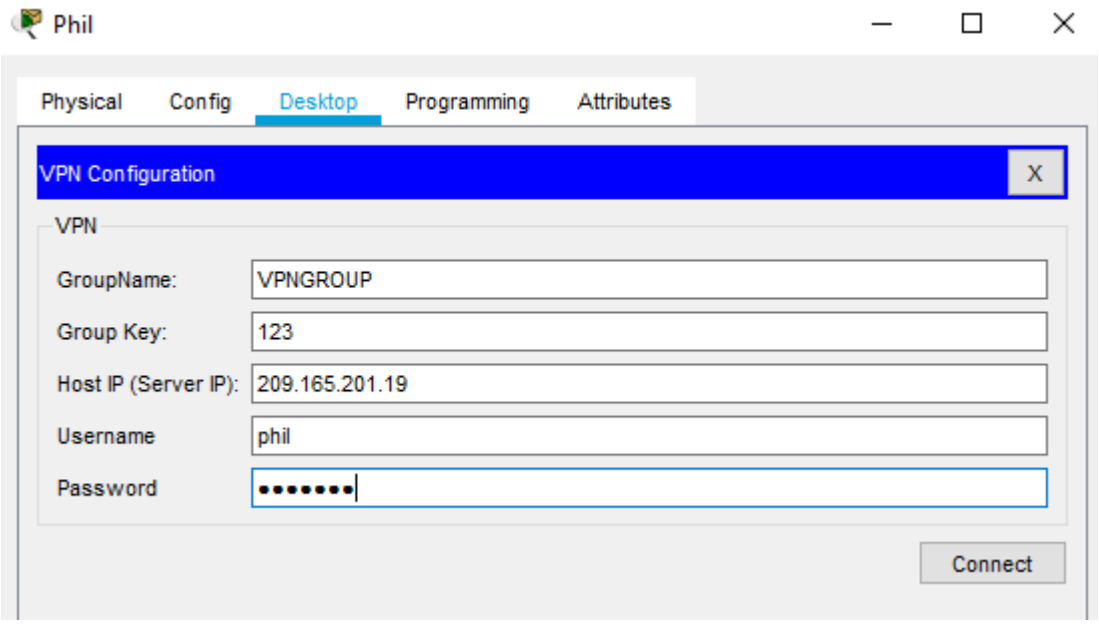
c. Type **quit** to exit **Public_FTP** server.

```
C:\>ping 209.165.201.19

Pinging 209.165.201.19 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 209.165.201.19: bytes=32 time=1ms TTL=253
Reply from 209.165.201.19: bytes=32 time=2ms TTL=253

Ping statistics for 209.165.201.19:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Part 2: Configuring the VPN Client on Phil's Computer

a. From **Phil's** computer, use the **ping** command and target the IP address of the **Branch_Router**. The first few pings may timeout. Enter the **ping** to get four successful pings.

b. On the **Desktop** tab, click on **VPN**



c. Within the **VPN Configuration** window, enter the following settings:

GroupName: ..... **VPNGROUP**

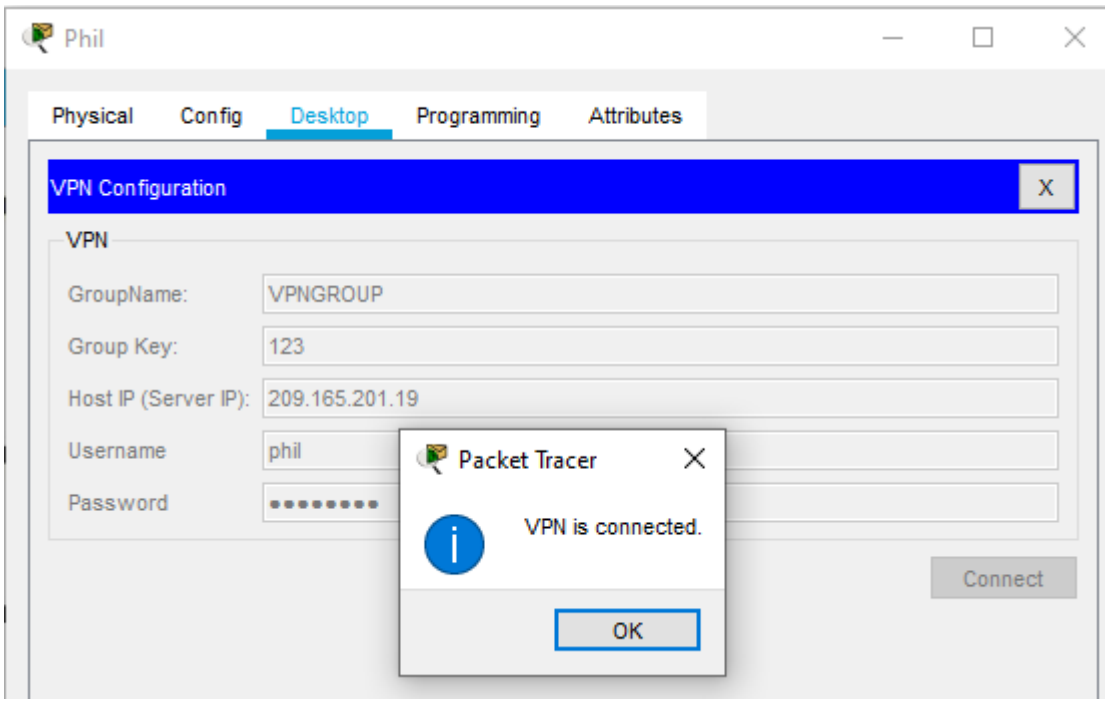
Group Key..... **123**

Host IP (Server IP):.. **209.165.201.19**

Username ..... **phil**

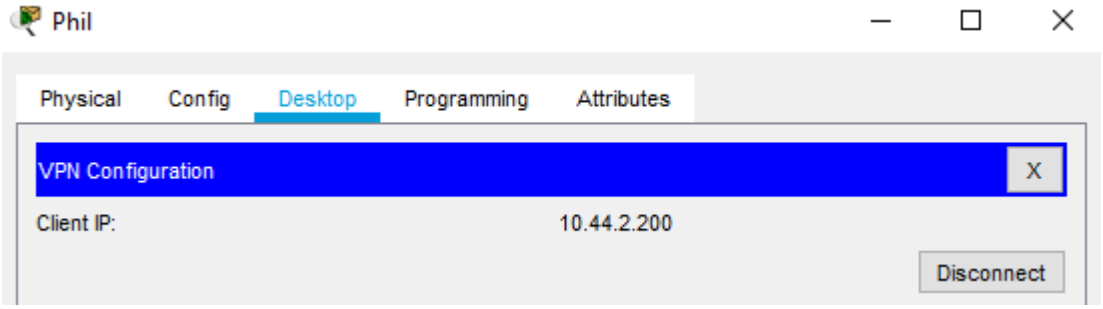
Password: **cisco123**

d. Click **Connect** and Click **OK** on the next window.



What is the Client IP for the client-to-site VPN connection?

10.44.2.200



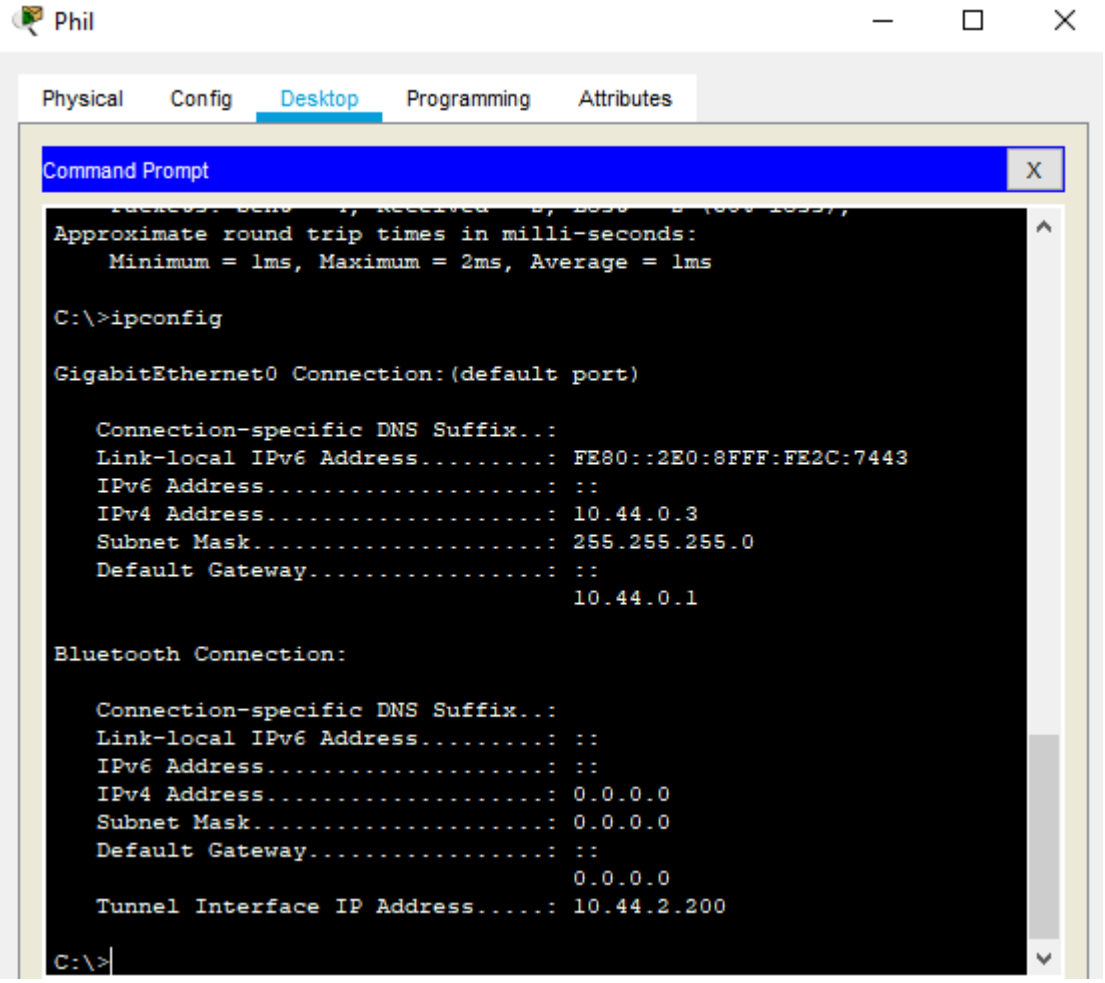
Part 3: Sending Encrypted FTP Traffic

Step 1: View the current IP addressing on Phil's computer.

a. Within the **Metropolis Bank HQ** site, click **Phil's** computer.

b. Click the **Desktop** tab and click on **Command Prompt**.

c. Use the **ipconfig** command to view the current IP address of **Phil's** PC.



What extra IP address is now shown that was not shown before in Part 1 Step 2c?

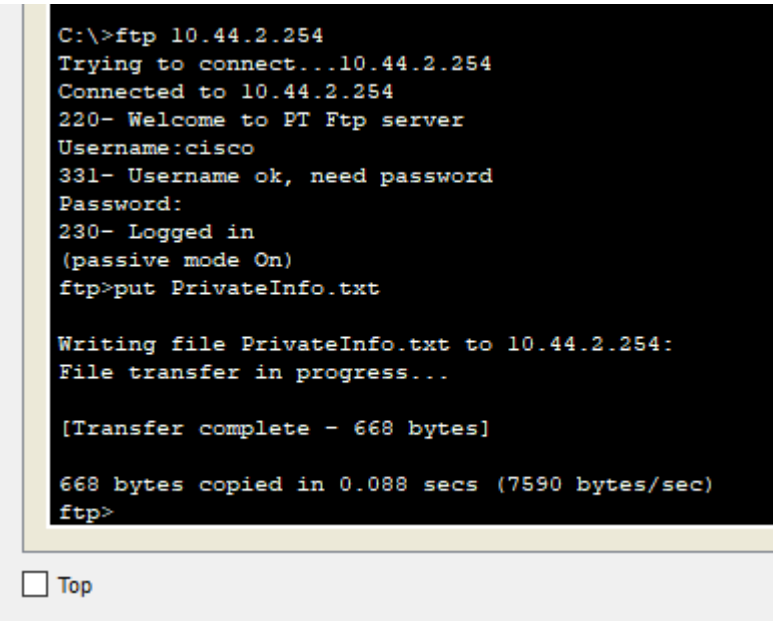
Tunnel Interface IP Address: 10.44.2.200

Step 2: Send encrypted FTP traffic from Phil's computer to the Private_FTP server.

a. Connect to the **Private_FTP** server at **Gotham Healthcare Branch** by entering **ftp 10.44.2.254** in the command prompt.

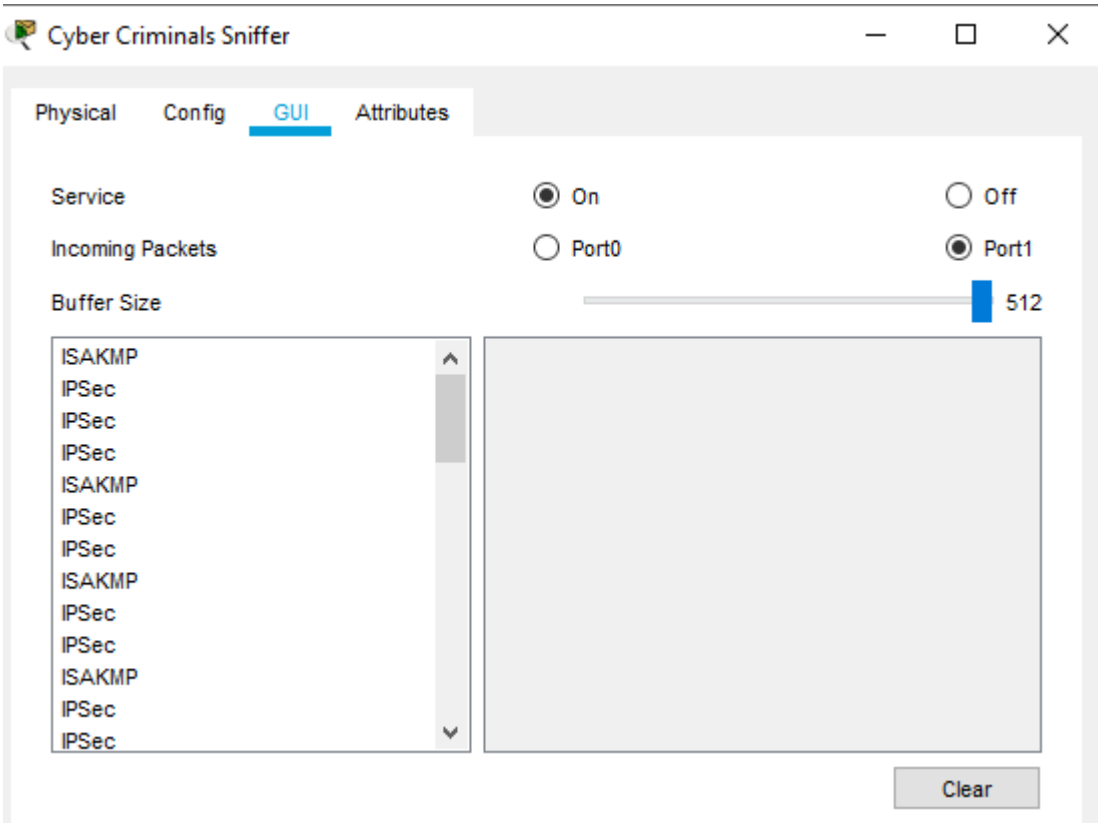
b. Enter the username of **cisco** and password of **secretkey** to login to the **Private_FTP** server.

c. Upload the file **PrivateInfo.txt** file to the **Private_FTP** server.



Step 3: View the traffic on the Cyber Criminals Sniffer

a. Maximize the **Cyber Criminals Sniffer** that was previously minimized.



b. Click the **FTP** messages displayed on the sniffer.

Are there any FTP messages displaying the password of internal or the file upload of PrivateInfo.txt?Explain.

No, the client-to-site VPN is using encryption and the Cyber Criminals Sniffer cannot decrypt the traffic to view it.