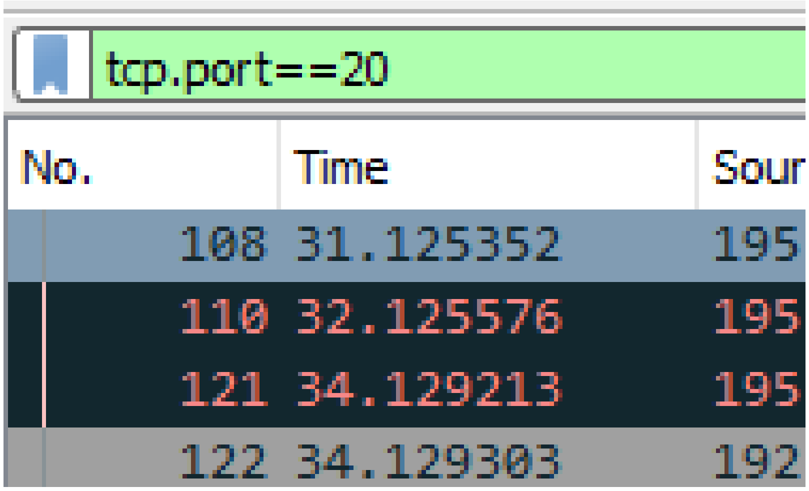
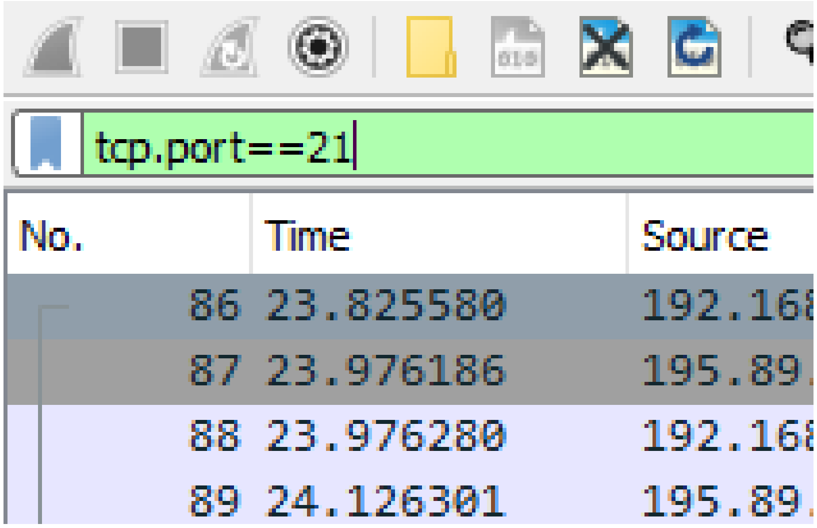
1



tcp.port==20

No.	Time	Sour
108	31.125352	195
110	32.125576	195
121	34.129213	195
122	34.129303	192

TCP Port 20 is used to transfer data.



tcp.port==21

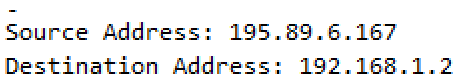
No.	Time	Source
86	23.825580	192.168
87	23.976186	195.89.
88	23.976280	192.168
89	24.126301	195.89.

TCP Port 21 is used to send commands and receive responses. First the connection is established through port 21 and after successful authentication, they can do communication.

2

This is the communication between a client and a server.Starting from the TCP handshake till the transfer of a file.

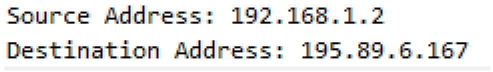
Packet No : 89



```
-
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The client pings the server to see if it's active or not. The server responds with 220 which means that the server is active.

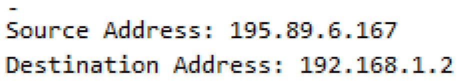
Packet No : 94



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client enters the username

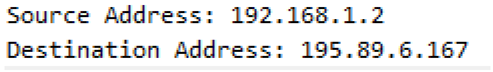
Packet No : 96



```
-
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server responds that it needs the password for the user account.

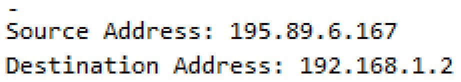
Packet No : 99



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client sends the password to the server

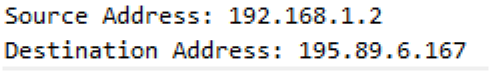
Packet No : 100



```
-
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server authenticates the user and grants access - The response code 230 tells that the user has successfully logged in.

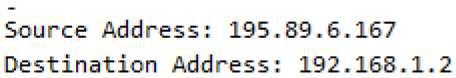
Packet No : 104



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client is telling the server which ip address and port it will use for transferring file/data

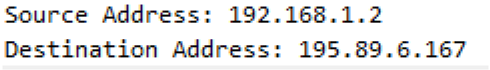
Packet No : 105



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server acknowledges and this means that the connection has been established without errors.

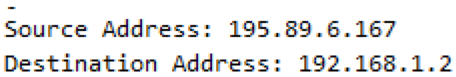
Packet No : 106



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client asks the server to send the list of files that it has available

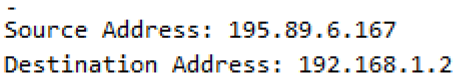
Packet No : 107



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

Status code 150 tells that the server is ready to open a data connection for transferring files and the ‘/’ indicates the root directory

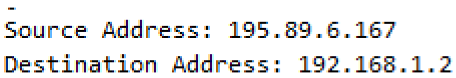
Packet No : 125



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server informs the client that a previous file transfer has completed successfully.

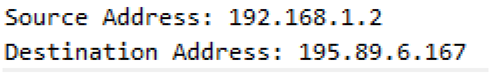
Packet No : 127



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

Server sends 125 bytes of data (likely a directory listing using the NLST command) to the client.

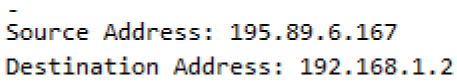
Packet No : 151



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client requests the server to connect to a specific port (PORT command)

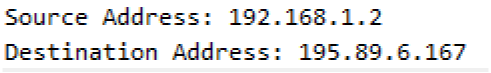
Packet No : 152



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server acknowledges the PORT command from the client and indicates it's ready for the data connection.

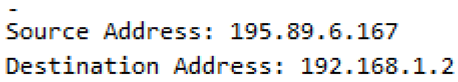
Packet No : 153



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client requests to retrieve a file named “legal.txt” from the server using the RETR command.

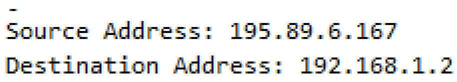
Packet No : 155



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server informs the client that it is opening a data connection in ASCII mode to start transferring legal.txt

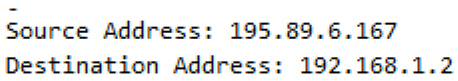
Packet No : 160



```
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server tells client that the file has been successfully transferred

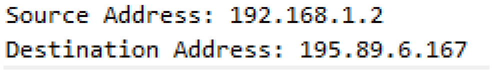
Packet No : 161



```
 -
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The server sends 1415 bytes of the requested file “legal.txt” to the client.

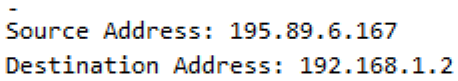
Packet No : 173



```
Source Address: 192.168.1.2
Destination Address: 195.89.6.167
```

The client sends a quit command to the server so that it can end the connection

Packet No : 175



```
 -
Source Address: 195.89.6.167
Destination Address: 192.168.1.2
```

The Server ends the connection and responds with a goodbye message

Lab Statement 2

1- Are ICMP messages sent over UDP or TCP?	TCP
2- What is the link-layer (e.g., Ethernet) address of the host?	c0:4a:00:87:05:fe
3- Which kind of request is sent through these ICMP packets?	Echo-request
4- How many requests are sent through the host?	4
5- What is the IP address of your host? What is the IP address of the destination host?	Src: 192.168.33.113 Dest: 172.217.27.36
6- Why is it that an ICMP packet does not have source and destination port numbers?	Since communicate between the network layer so there is no need for port that are utilized by application-layer
7- What values in the ICMP request message differentiate this message from the ICMP reply message?	First Bytes has the type:8 for request msg while type:0 for reply msg

8- Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	Type:8 Code :0 2 bytes is the size for Checksum, sequence number and identifier field.
9- Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?	Type:0 Code:0 2 bytes is the size for Checksum, sequence number and identifier field.
10-Examine the packet no 56. What are the ICMP type and code numbers? Why is the IP and TCP Header included in the ICMP Header? What does these headers depict?	Type:3 Code:3 ICMP is used for diagnostics purposes and it includes these headers so a user can debug the issue in communication.

Lab Statement 3

a. What is a packet sniffer in computer networks, and how does it function?
A packet sniffer is a hardware or software tool designed to monitor network traffic. Since data is transmitted in packets, a packet sniffer inspects the flow of these packets between clients and servers.

b. What is the main purpose of tools like Wireshark in network troubleshooting and monitoring?
Wireshark is primarily used to monitor and analyze network traffic to help identify and resolve issues, as well as to uncover potential network vulnerabilities.

c. In Wireshark, what is the importance of a "capture filter," and when would you use it during packet capture?
A capture filter helps narrow down the packet data being captured by allowing users to specify conditions, such as focusing on a particular protocol or port. This makes it easier to capture only relevant traffic.

d. What is a potential ethical concern related to the use of packet sniffers in network security and privacy?
The use of packet sniffers raises privacy concerns because they can intercept sensitive information, such as passwords or personal data, leading to unauthorized access and information theft.

e. What are some common protocols or technologies that Wireshark can analyze and decode in captured packets? Give examples.
Wireshark can capture traffic from various sources like Bluetooth, Ethernet, and Wi-Fi. It supports analyzing several protocols, including HTTP, FTP, UDP, and TCP.