Muhammad Laraib Akhtar

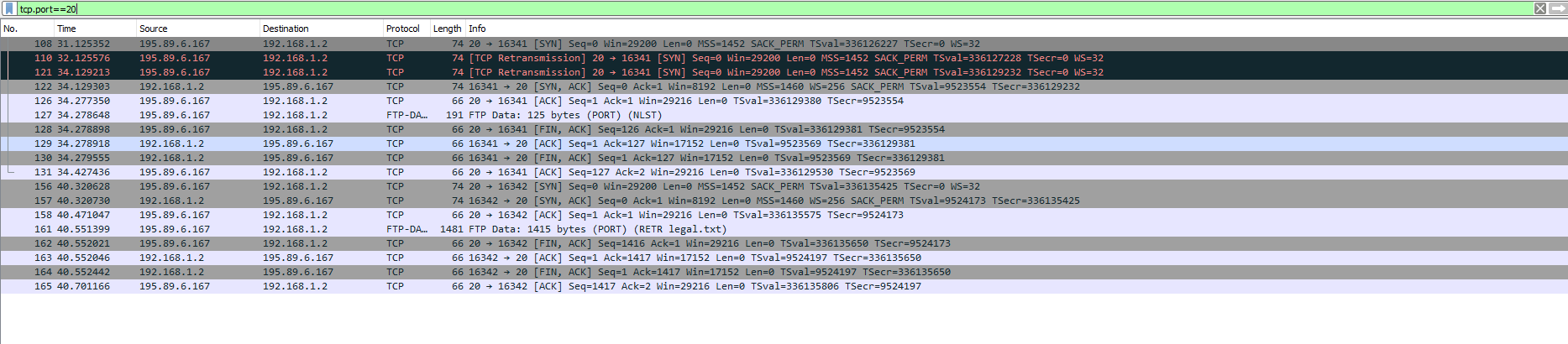
BCS-5B1

21L-5294

Lab-4

**Use the FTP\_Session.pcapng (Wireshark Capture File) to answer the questions below**

1. FTP uses two port numbers: 20 and 21. Apply **tcp.port==20** and **tcp.port==21**. Analyze the result and write down the purposes of these two ports for FTP.



A screenshot of a computer

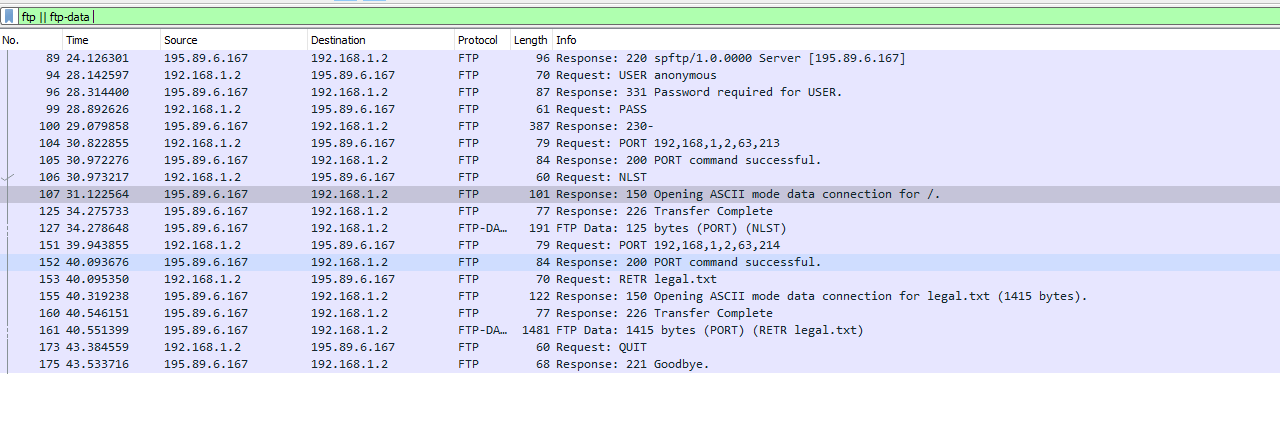
Description automatically generated

Port 21 is known as the control port in FTP. It is used for the control channel of the FTP connection.

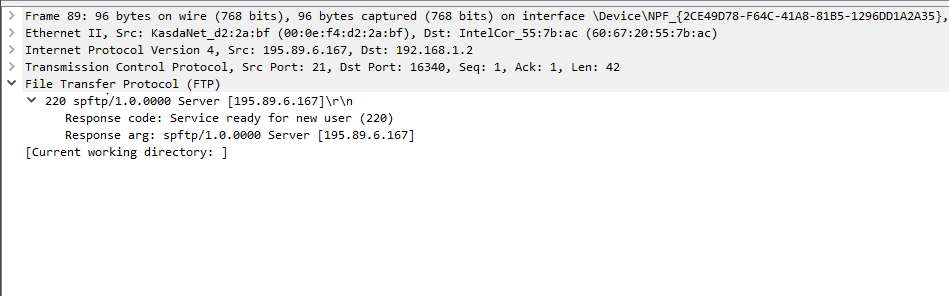
Port 20 is the data port in FTP. It is used for the actual data transfer during FTP sessions.

1. Filter out each packet using either FTP or FTP-DATA Protocol (using **ftp || ftp-data** filter). Mention each packet number and its purpose with reference to request made and response received in the above mentioned FTP Session in command line to get file legal.txt (screenshot show above). Also look for **Response Code** and **Response Arg** in the FTP Header for each packet

**(**There are **19 such packets** and you have to write one/two lines explanation for each packet, what the packet is doing w.r.t FTP Session (Screenshot shown above) **e.g., Packet 104: Client asks server to send the data on IP:192.168.1.2 and Port:16341** [63(0x3F),213(0xD5) and **(0x3FD5=16341**)**] )**



Packet 89, server response to client IP: 192.168.1.2 and Port 16340



Packet 94, client request server IP: 195.89.6.167 and Port 21

A screenshot of a computer

Description automatically generated

Packet 96, server response to client IP: 192.168.1.2 and Port 16340

A screenshot of a computer

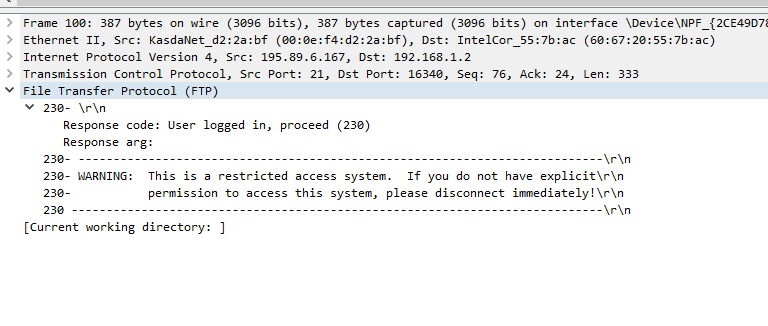
Description automatically generated

Packet 99, client request server IP: 195.89.6.167 and Port 21

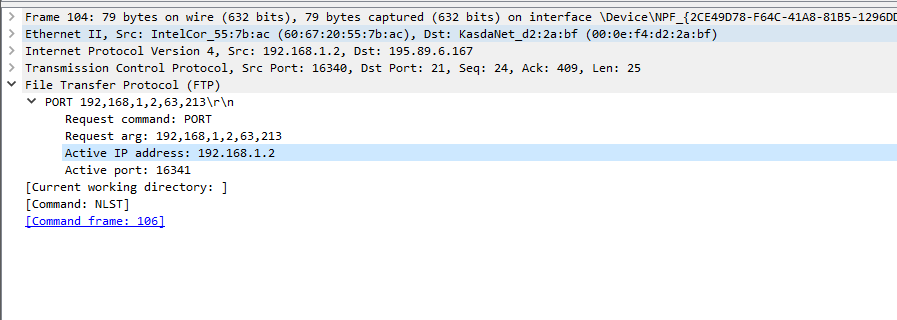
A screenshot of a computer

Description automatically generated

Packet 100, server respond client IP: 192.168.1.2 and Port 16340



Packet 104: Client request server to send the data on IP:192.168.1.2 and Port:16340



Packet 105: Server response to client on IP:192.89.6.167 and Port:21

A screenshot of a computer

Description automatically generated

Packet 106: Client request server to send the data on IP:192.168.1.2 and Port:16340

A screenshot of a computer

Description automatically generated

Packet 107: Server response to client on IP:192.89.6.167 and Port:16340

A screenshot of a computer

Description automatically generated

Packet 125: Server response to client on IP:192.89.6.167 and Port:16340

A computer screen shot of a computer

Description automatically generated

Packet 127: server sends client data from Ip: 195.89.6.167 and port 20.

A screenshot of a computer

Description automatically generated

Packet 151: client requests server data from IP:192.168.1.2 and port 16340.

A screenshot of a computer

Description automatically generated

Packet 152: server sends response from Ip: 195.89.6.167 and port 21.

A screenshot of a computer program

Description automatically generated

Packet 153: client requests server to send data from Ip: 192.168.1.2 and port 16340.

A screenshot of a computer

Description automatically generated

Packet 155, server sends client data from IP:195.89.6.167 and port 21

A screenshot of a computer

Description automatically generated

 Packet 160, server sends client data from IP:195.89.6.167 and port 21

A screenshot of a computer

Description automatically generated

Packet 161, server sends client data from IP:195.89.6.167 and port 20

A screenshot of a computer

Description automatically generated

Packet 173, client asks server to send the data on IP:192.168.1.2 and port 16340

A screenshot of a computer

Description automatically generated

 Packet 175, server sends client data form IP: 195.89.6.167 and port 21

A screenshot of a computer

Description automatically generated

**Lab Statement 2: Analyzing ICMP Packets using Wireshark (5)**

* + **Step 1:** Run Wireshark
  + **Step 2:** Load the Session file **ICMP\_Session**
  + **Step 3:** Now filter out all non-ICMP packets by typing “icmp” (without quotes) in the filter field towards the top of the Wireshark window
  + **Step 4:** Analyze the ICMP Packets and answer the following questions

1.Are ICMP messages sent over UDP or TCP?

ICMP (Internet Control Message Protocol) messages are not sent over either UDP (User Datagram Protocol) or TCP (Transmission Control Protocol). ICMP is a separate network layer protocol that operates directly over the Internet Protocol (IP) layer.

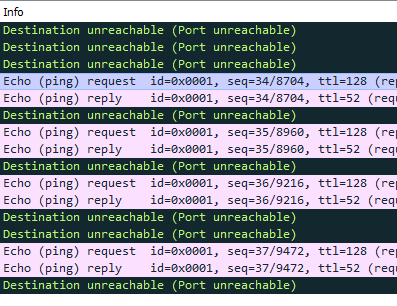
2.What is the link-layer (e.g., Ethernet) address of the host?



1. Which kind of request is sent through these ICMP packets?

ICMP (Internet Control Message Protocol) packets are used to send various types of control and error messages between network devices. Some common types of ICMP requests and messages include:

1. **Echo Request and Echo Reply (Ping)**.
2. **Destination Unreachable**.
3. **Time Exceeded** etc.



1. How many requests are sent through the host?

A screenshot of a computer program

Description automatically generated

4 requests are sent from the host.

1. What is the IP address of your host? What is the IP address of the destination host?

Source host:192.168.33.110

Destination host:172.217.27.36

1. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP (Internet Control Message Protocol) packets do not have source and destination port numbers because ICMP operates at a different layer of the network stack compared to protocols like TCP and UDP. ICMP and TCP/UDP serve different purposes in the network stack. ICMP is focused on network control and diagnostics, while TCP and UDP are used for end-to-end application data transfer. As a result, ICMP packets lack the concept of source and destination port numbers, which are specific to transport layer protocols like TCP and UDP.

1. What values in the ICMP request message differentiate this message from the ICMP reply message?

Request: The Type field is set to 8



Reply: The Type field is set to 0



1. 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?

A screenshot of a computer

Description automatically generated

1. 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?

A screenshot of a computer program

Description automatically generated

1. 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?

The IP and TCP headers are not included within the ICMP header; rather, ICMP messages are encapsulated within IP packets, and the IP and TCP headers provide necessary information for routing and delivering the ICMP packet. By including these headers, the ICMP message provides detailed information to the sender about why a particular packet was unreachable or encountered an issue. It helps in diagnosing network problems and understanding the specific cause of the problem.

