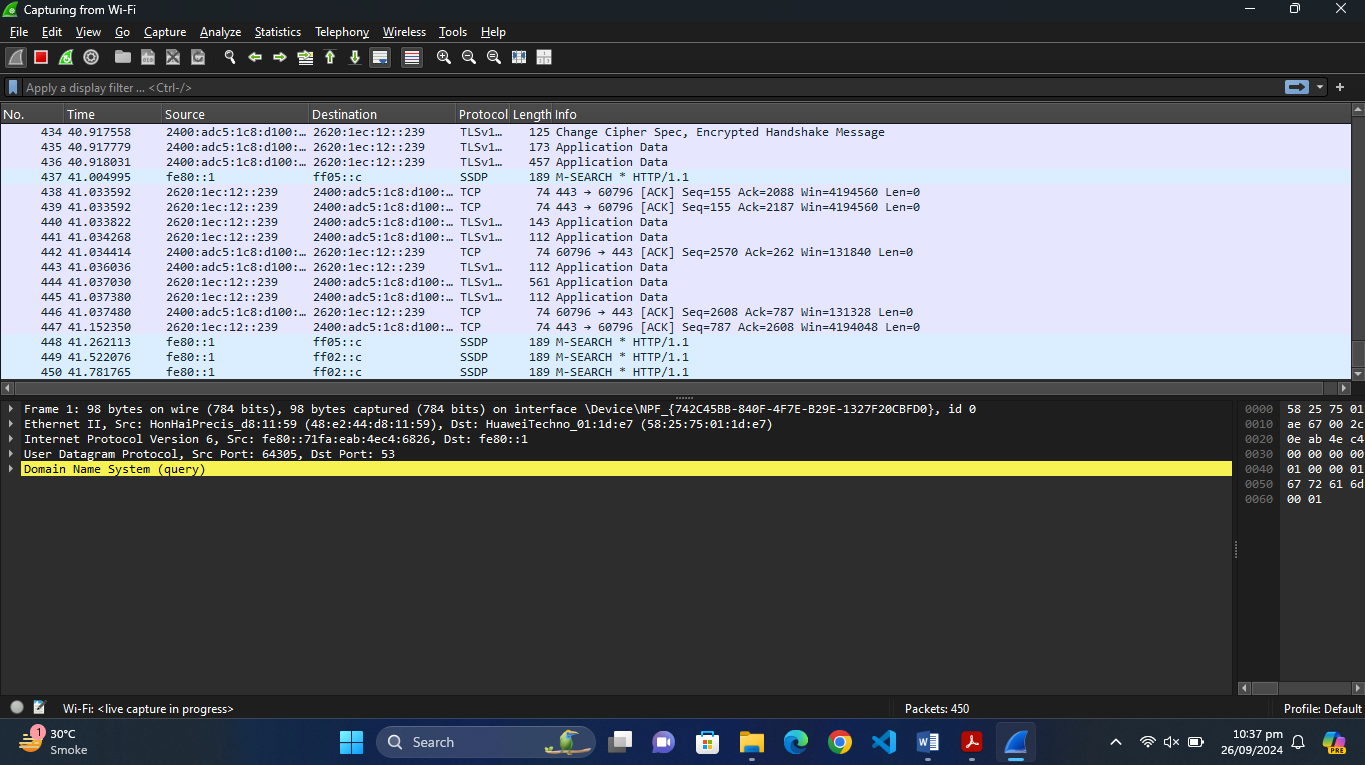
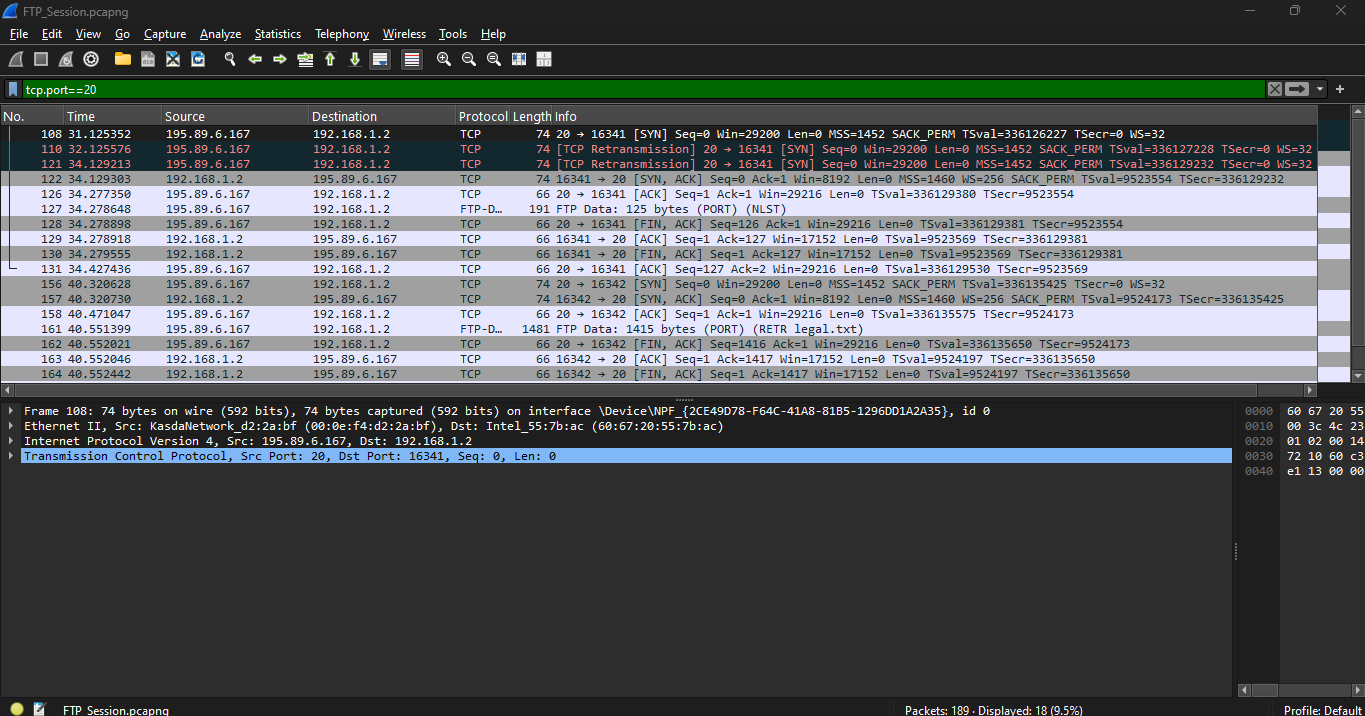
**Lab Statement 1: Capturing FTP packets using Wireshark**

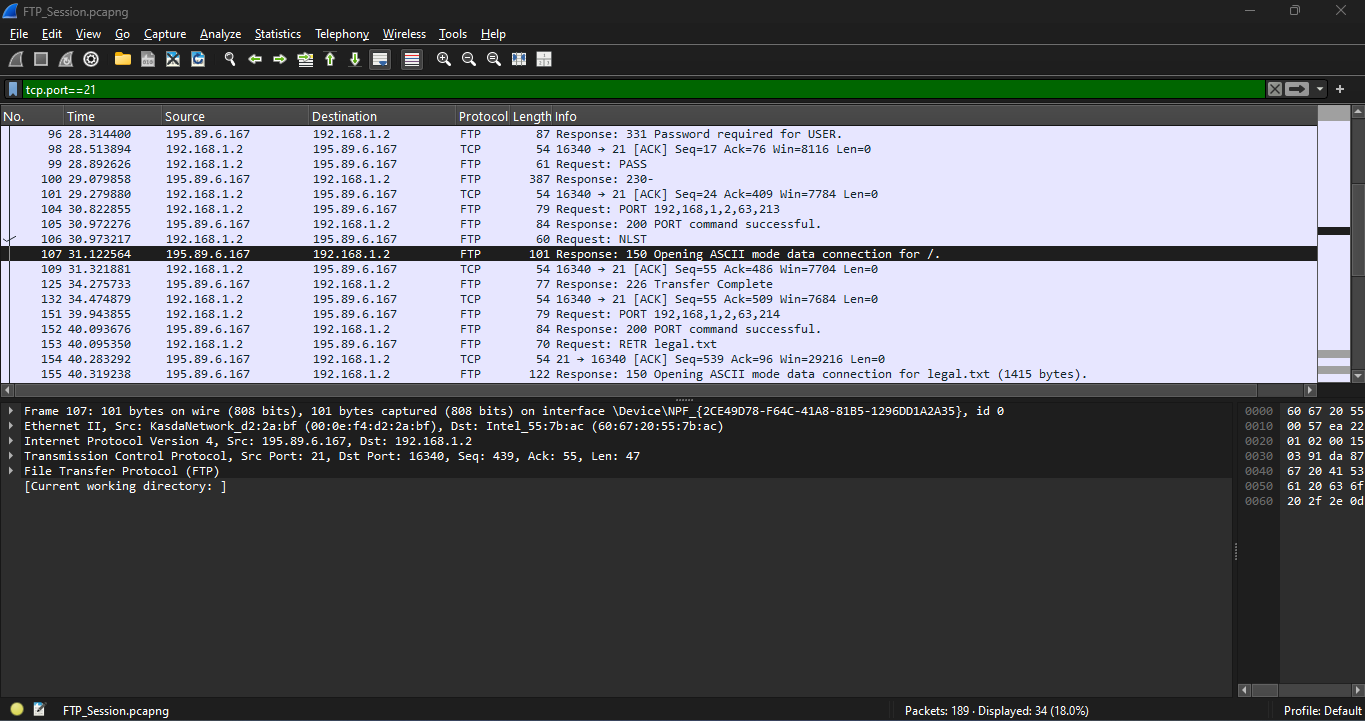
Closed all the unnecessary traffic



1. Port 20:



Port 21:



Analysis:

All the packets with tcp ports 20 and 21 are displayed according to the filter.

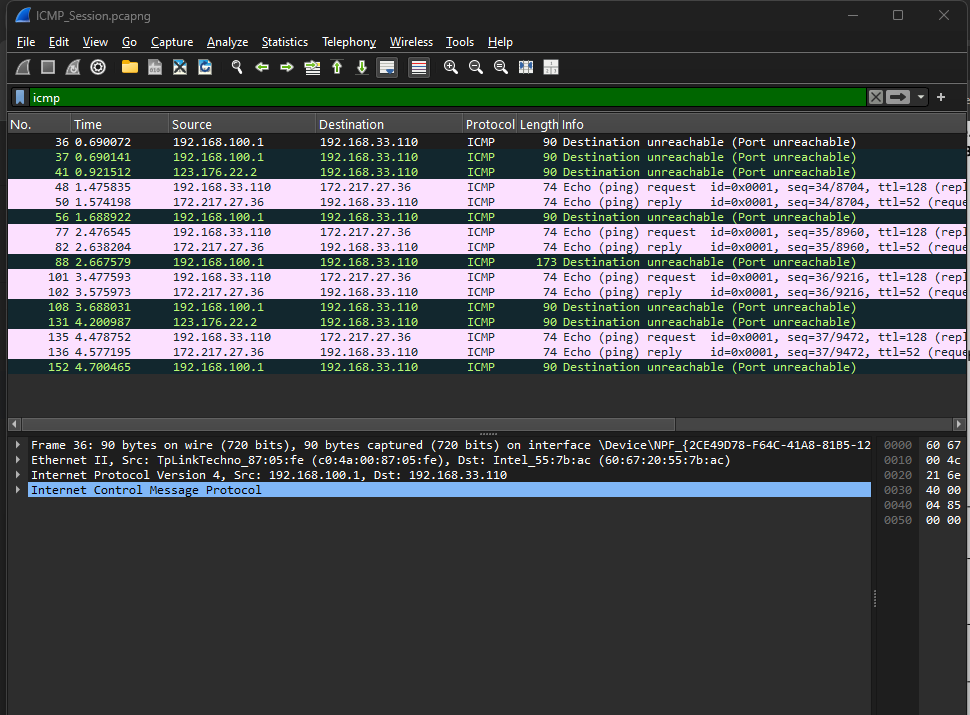
Purpose:

* Port 20 is also known as a data port and is used for transferring data between the servers and clients.
* Port 21 is also known as the control port and is used for sending commands between clients and servers.

1. The following is the information required for the 19 packets gained from applying the filter ftp||ftp-data:

* Packet 89: Server responses to the request of the user on IP:195.89.6.167 and Port:21 with response code: 20
* Packet 94: Client requests the server to login the user on IP: 192.168.6.167 and Port: 16340 with the request message: USER anonymous
* Packet 96: Server responses to the request of client on IP: 195.89.6.167 and Port:21 with response code :331(Password requirement)
* Packet 99: Client requests to authenticate the password on I{“192.168.1.2 and Port: 16340 with request message “PASS”
* Packet 100: servers’ responses to the client on IP:192.189.6.167 and Port:21 with request code 230
* Packet 104: Client requests the server to send data on IP: 192.168.1.2 and Port: 16340
* Packet 105: Server responses to the client on IP: 195.89.6.167 and Port: 21 with response code:200
* Packet 106: Client requests the server on IP: 192.168.1.2 on Port:16340 and Port:16340 with request command “NLST”
* Packet 107: Server responses to the client on IP: 195.89.6.167 and Port: 21 with response code:150
* Packet 125: Server responses to the client on IP: 195.89.6.167 and Port: 21 with response code:226
* Packet 127: FTP Data on the IP:195.89.6.167 and Port:20
* Packet 151: Client requests the server on IP: 192.168.1.2 and Port: 16340
* Packet 152: Server responses to the client on IP: 195.89.6.167 and Port: 21 with response code:200
* Packet 153: Client requests the server on IP: 192.168.1.2 on Port:16340 and Port:16340
* Packet 155: Server responses to the client on IP: 195.89.6.167 and Port: 21 with response code:122
* Packet 160: Server responses to the client on IP: 195.89.6.167 and Port: 21 with response code:226
* Packet 161: FTP Data on the IP:195.89.6.167 and Port:20
* Packet 173: Client requests the server on IP: 192.168.1.2 on Port:16340 and Port:16340 with request command “QUIT”.
* Packet 175: Server responses the client on IP:195.89.6.167on Port:21 and response code: 221

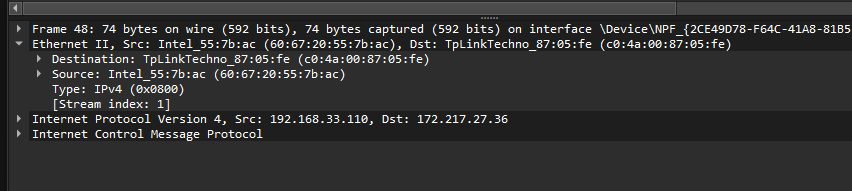
**Lab Statement 2: Analyzing ICMP Packets using Wireshark**



**1- Are ICMP messages sent over UDP or TCP?**

ICMP stands for Internet Control Message Protocol. ICMP is itself a protocol so it doesn’t need any other protocol to send messages.

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



Source: TpLinkTechno\_87:05:fe (c0:4a:00:87:05:fe)

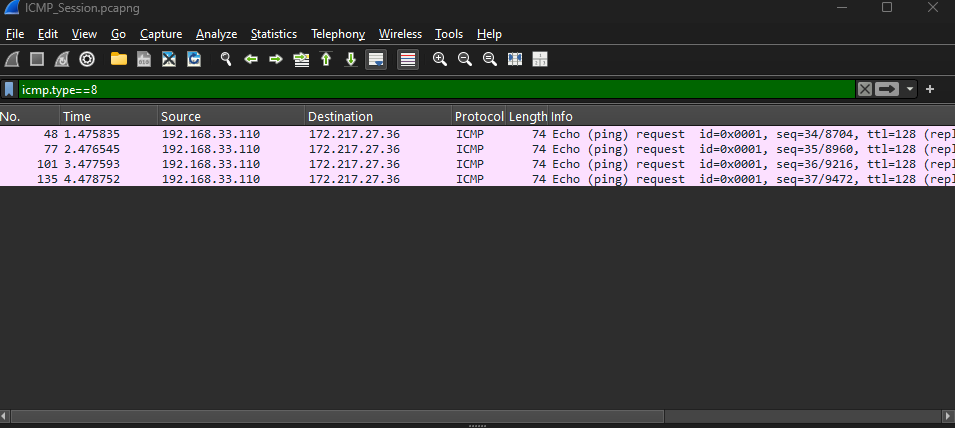
Destination: Intel\_55:7b:ac (60:67:20:55:7b:ac)

**3- Which kind of request is sent through these ICMP packets?**

Echo (ping) request

**4- How many requests are sent through the host?**

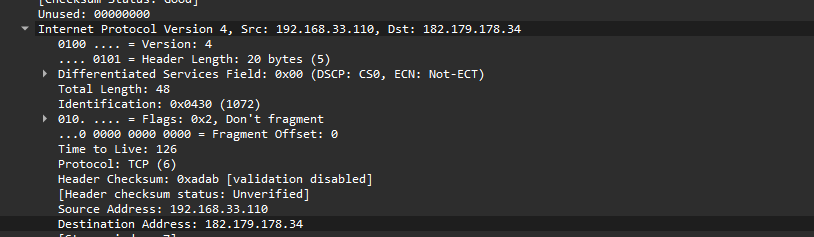
4 requests are sent through the host



**5- What is the IP address of your host? What is the IP address of the destination host?**

Source Address: 192.168.33.110 (Host)

Destination Address: 182.179.178.34



**6- Why is it that an ICMP packet does not have source and destination port numbers?**

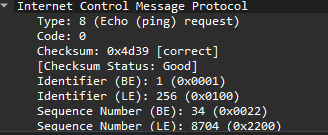
ICMP is a network layer protocol. It deals with error handling and diagnosis of the network. Moreover, these tasks don’t need any port number. That is the reason for not having port numbers as it is not used for communication.

**7- What values in the ICMP request message differentiate this message from the ICMP reply message?**

The type is the value factor that differentiates the both. The request message has type 8 whereas the reply message has type 0.

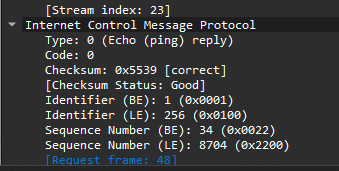
**8- Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

* ICMP type: 8
* Code numbers: 0
* Identifiers, Checksums and sequence numbers are 2 bytes.



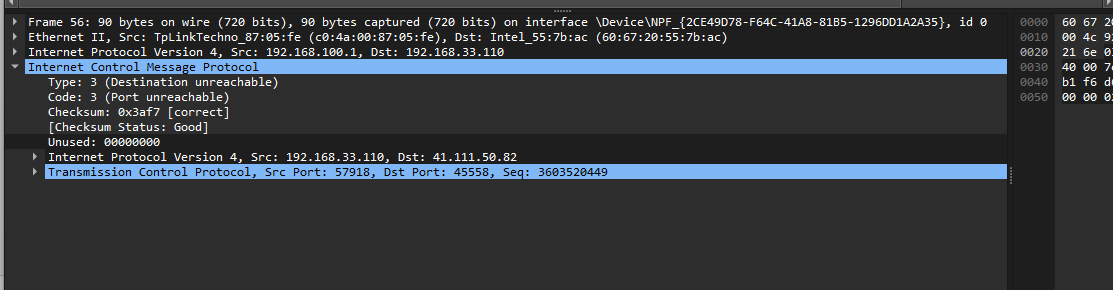
* It doesn’t have other fields in the file, but it can have fields like payload, payload length, timestamp, header checksum, etc.

**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?**



* ICMP type: 0
* Code: 0
* The identifier, checksum, and sequence number are 2 bytes.
* The other fields include all the fields that the request message has for example, checksum header, flags, total length, etc.

**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?**



* ICMP type: 3
* Code: 3
* The purpose of the IP header is to provide the router and delivery information for the packets that include ICMP. It includes source and destination IP address, version, total length, TTL, etc.
* The TCP header is included only when it is used for the communication. It provides source and destination ports, checksum, sequence number, flags, etc.