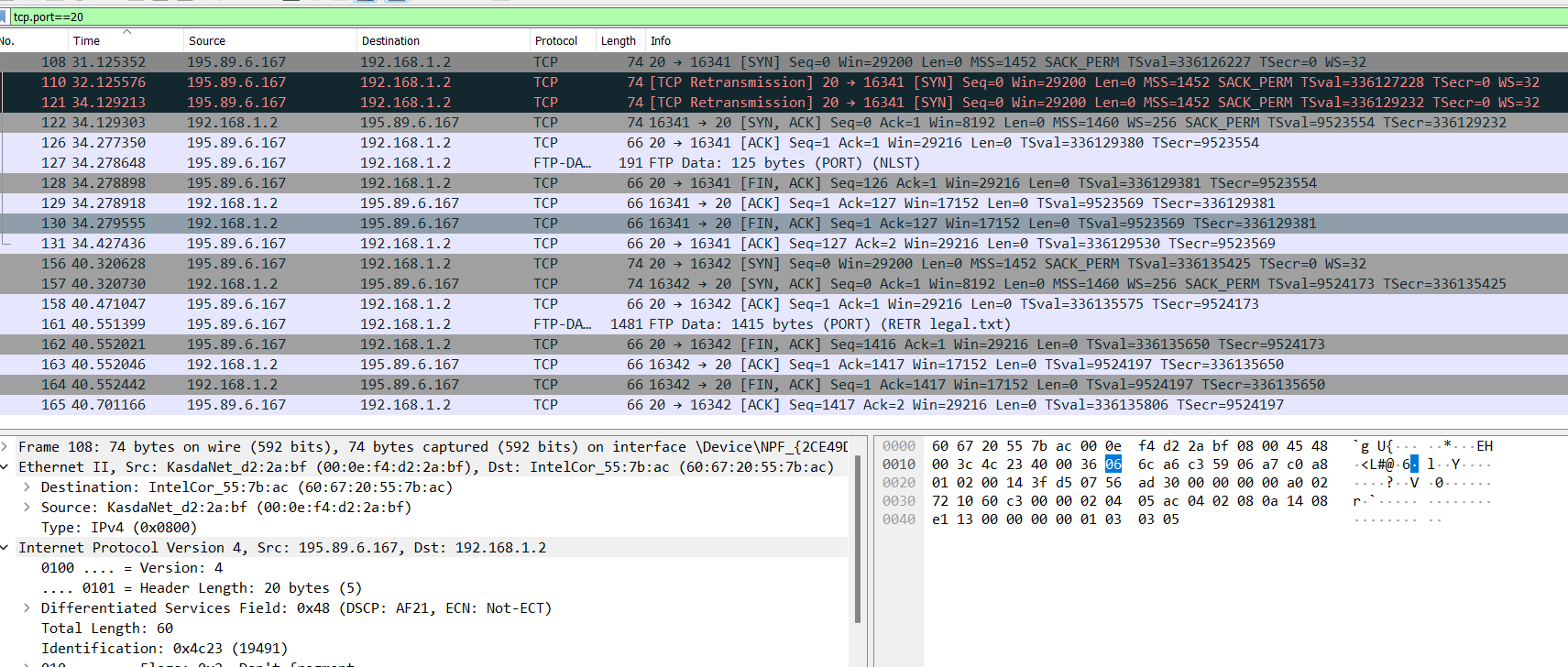
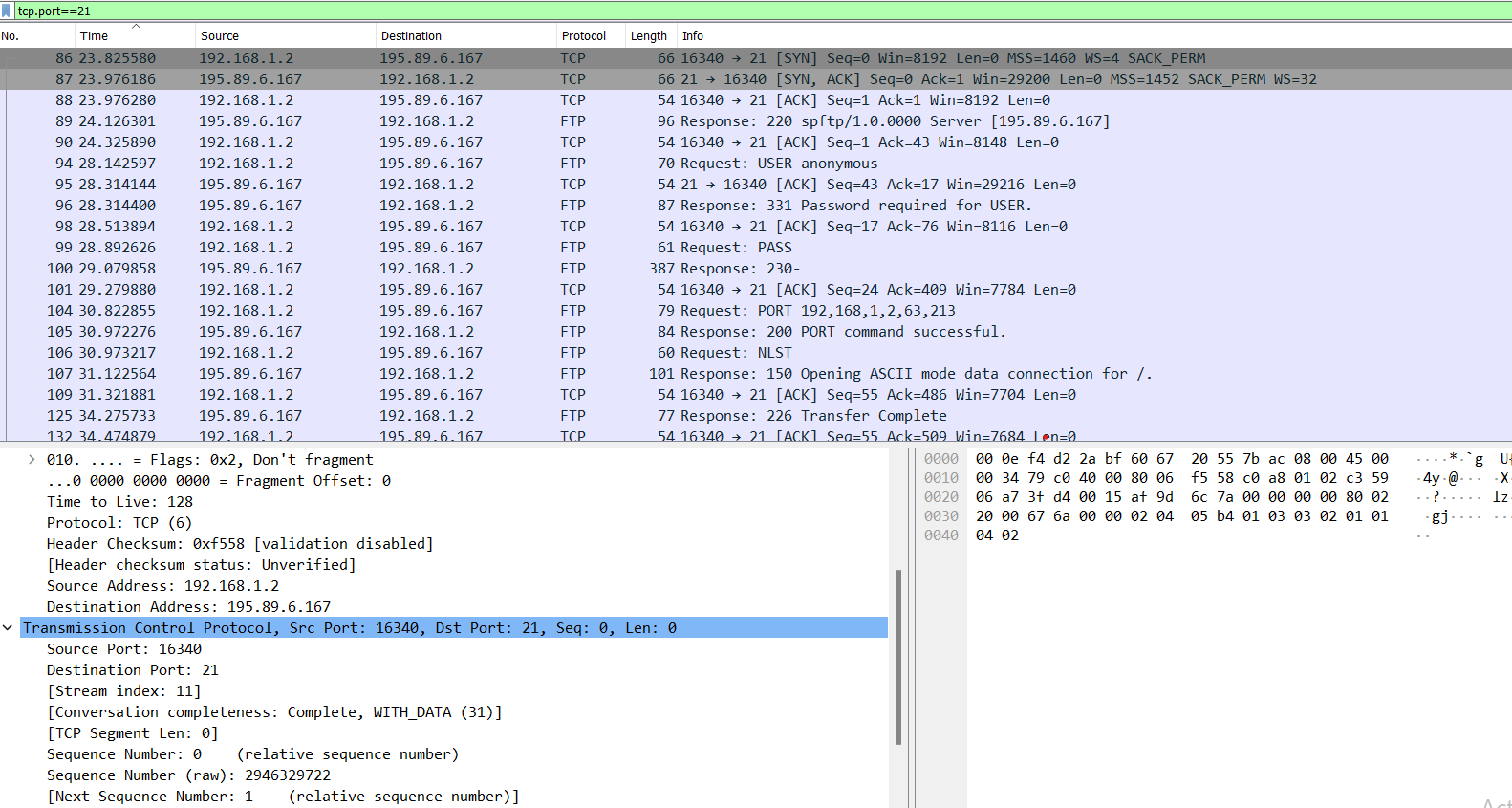
**Lab 4**

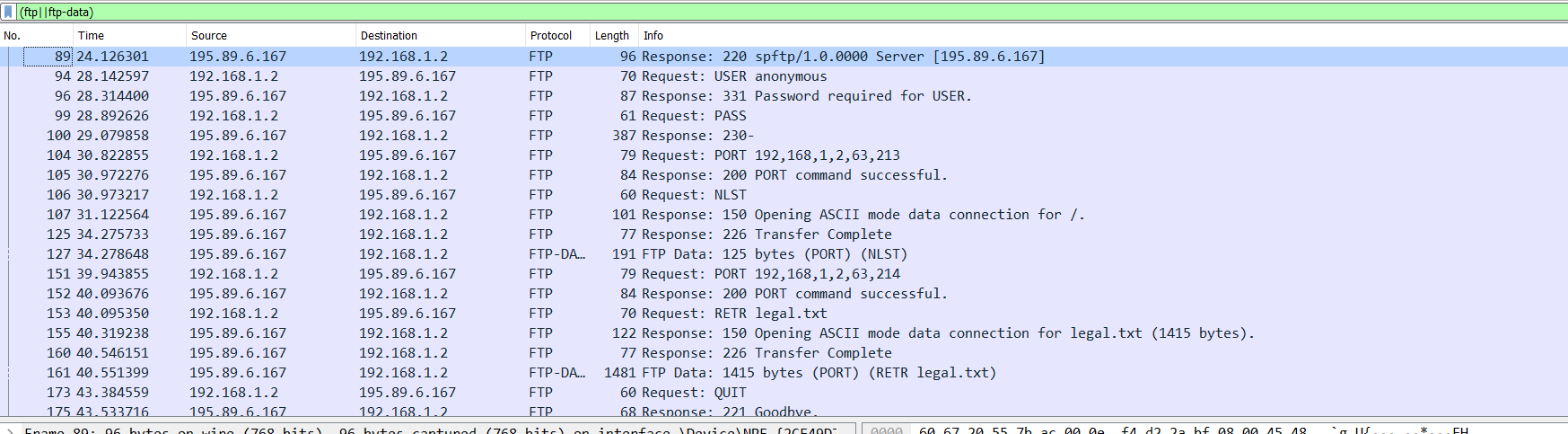
**Question 1:**

Tcp port 20 is used to transfer data between client and server whereas Tcp port 21 is used to establish the connection between client and server.





**Question 2**

  
  
**Packet 89**: FTP source (ip.src == 195.89.6.167) send a ‘Response 220’ packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340

**Packet 94**: FTP source (ip.src == 192.168.1.2) send a ‘Request: USER anonymous’ message to destination (ip.dst == 195.89.6.167) . The message is that the ‘USER anonymous’. It basically tells that the username is anonymous. It is sent from port number 16340 to 21

**Packet 96**: FTP source (ip.src == 195.89.6.167) send a ‘Response: 331 Password required for USER.’ packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340

**Packet 99:** FTP source (ip.src == 192.168.1.2) send a ‘Request: PASS’ message to destination (ip.dst == 195.89.6.167). The message is that the password is ‘ ’. It is sent from port number 16340 to 21

**Packet 100:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 230’( which tells that the login is proceeded) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340

**Packet 104**: FTP source (ip.src == 192.168.1.2) send a ‘Request: PORT 192,168,1,2,63,213’ message to destination (ip.dst == 195.89.6.167) . It is sent from port number 16340 to 21. It asks server to send the data on ip 192.168.1.2

**Packet 105:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 200 PORT command successful.’ (which tells that the PORT command is successful) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

**Packet 106:** FTP source (ip.src == 192.168.1.2) send a NLST request ‘Request: NLST’ message to destination (ip.dst == 195.89.6.167). It is sent from port number 16340 to 21. It asks to retrieve a list of files from server.

**Packet 107:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 150 Opening ASCII mode data connection for /’ (which tells that it is opening new connection to send ASCII mode data) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

**Packet 125:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 226 Transfer Complete’ (which tells that the transfer is completed and it is closing data connection) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

**Packet 127:** FTP source (ip.src==195.89.6.167) transfers 125 bytes of data through FTP-DATA protocol TCP port 20 to FTP destination (ip.dst==192.168.1.2). Source Port 20 and destination port 16341.

**Packet 151:** FTP source (ip.src == 192.168.1.2) send a ‘Request: PORT 192,168,1,2,63,214’ message to destination (ip.dst == 195.89.6.167) . It is sent from port number 16340 to 21. It asks server to send the data on ip 192.168.1.2

**Packet 152:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 200 PORT command successful’ (which tells that the PORT command is successful) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

**Packet 153:** FTP source (ip.src == 192.168.1.2) send a ‘Request: RETR legal.txt’ message to destination (ip.dst == 195.89.6.167) . It is sent from port number 16340 to 21. It requests to retrieve/ download legal.txt file from server.

**Packet 155:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 150 Opening ASCII mode data connection for legal.txt’ (which tells that is opening new connection to send ASCII mode data for legal.txt file) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

**Packet 160:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 226 Transfer Complete’ (which tells that the transfer is completed and it is closing data connection) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

**Packet 161:** FTP source (ip.src ==195.89.6.167) transfers 1415 bytes of data through FTP-DATA protocol TCP port 20 to FTP destination (ip.dst==192.168.1.2) consisting of legal.txt. Source port number 20 and destination 16342.

**Packet 173:** FTP source (ip.src == 192.168.1.2) send a ‘Request: QUIT’ message to destination (ip.dst == 195.89.6.167) . It is sent from port number 16340 to 21. It requests to end the user session.

**Packet 175:** FTP source (ip.src == 195.89.6.167) send a ‘Response: 221 Goodbye’ (which tells that the service is closing control connection) packet to destination (ip.dst == 192.168.1.2) with source port number 21 and destination 16340.

Question 2

|  |
| --- |
| 1. Are ICMP messages sent over UDP or TCP?     They are not sent over TCP or UDP, they have their own protocol. |
| 1. What is the link-layer (e.g., Ethernet) address of the host?     Source: Tp-LinkT\_87:05:fe (c0:4a:00:87:05:fe)  Destination: IntelCor\_55:7b:ac (60:67:20:55:7b:ac) |
| 1. Which kind of request is sent through these ICMP packets?     Type: 8 request which is used for ping requests |
| 1. How many requests are sent through the host?   4 requests are sent through the host. |
| 1. What is the IP address of your host? What is the IP address of the destination host?     The IP Address of the host is: 192.168.33.100  The IP Address of the Destination is: 172.217.27.36 |
| 1. Why is it that an ICMP packet does not have source and destination port numbers?   ICMP operates at the network layer, it doesn't require source and destination port numbers. |
| **7-** What values in the ICMP request message  differentiate this message from the ICMP reply message?  The Type field helps in differentiating the request and reply message from each other. |
| 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?   ICMP Type number is 8 (ECHO (ping) request) with code 0. It contains Checksum, Checksum Status, Identifier (BE & LE), Sequence Number (BE & LE). Checksum, Identifier and Sequence fields are of 2 bytes each. |
| **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 number 0 (ECHO (ping) reply) with code 0. It contains Checksum, Checksum Status, Identifier (BE & LE), Sequence Number (BE & LE). Checksum, Identifier and Sequence fields are of 2 bytes each. |
| **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?    So, when packet fails it generates an ICMP destination unreachable and port unreachable message (type 3, code 3). To tell the sender more about the error ICMP message include first 8 bytes of original IP packet’s header and some portion of payload. The first 8 bytes of IP header includes source and destination IP addresses and other information. The portion of payload includes source and destination port numbers. So, IP header depicts source and destination IP addresses and TCP header depicts source and destination port numbers |