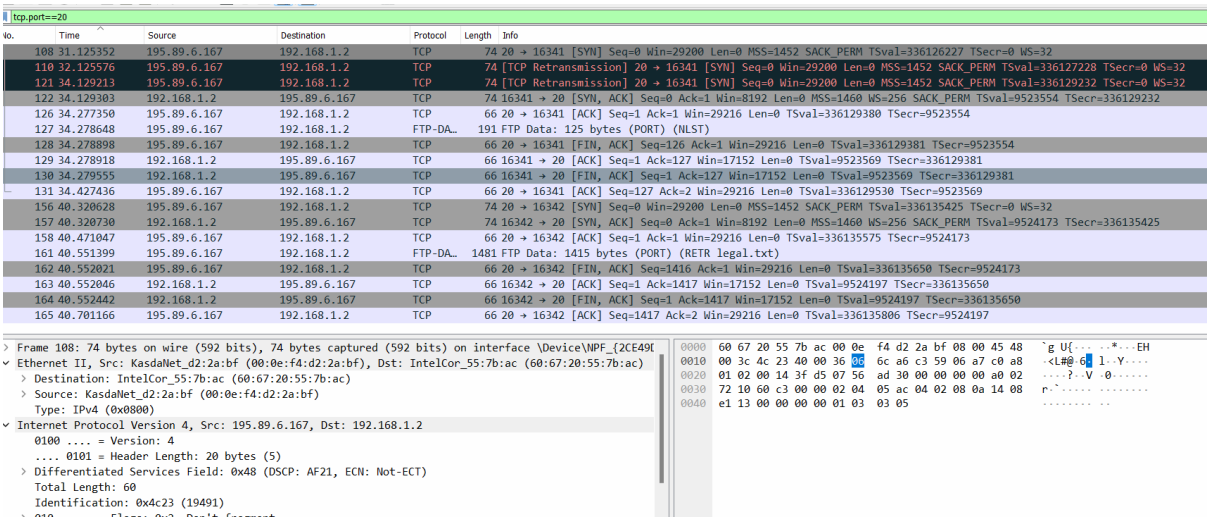
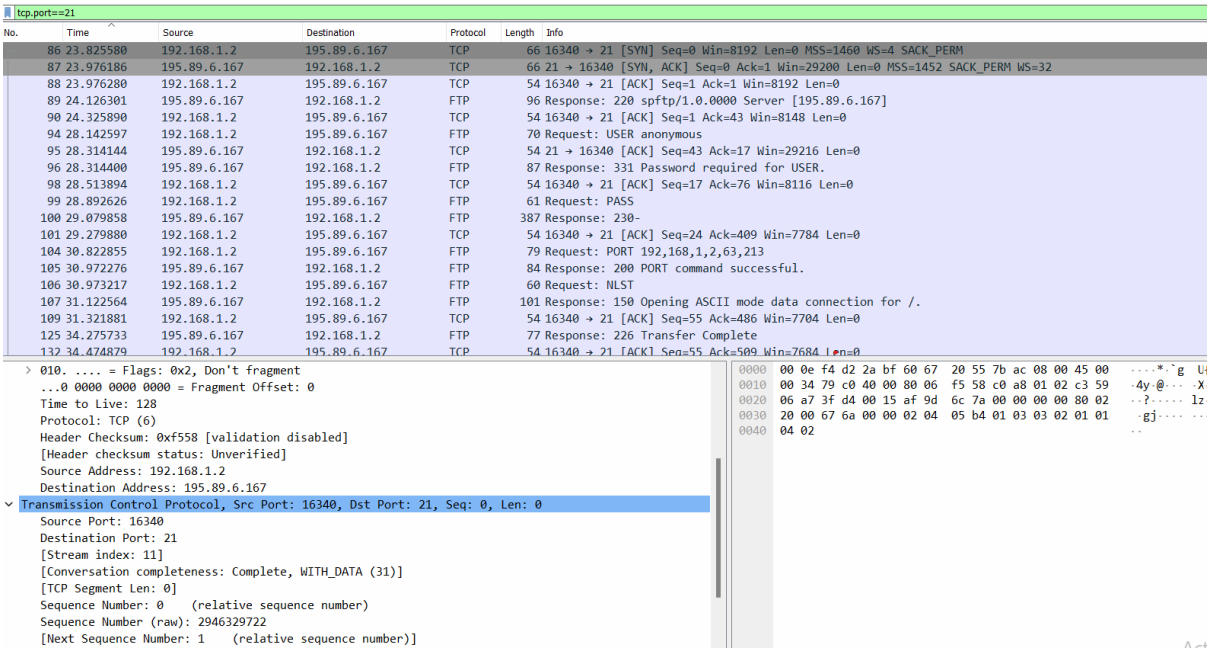
Lab 4

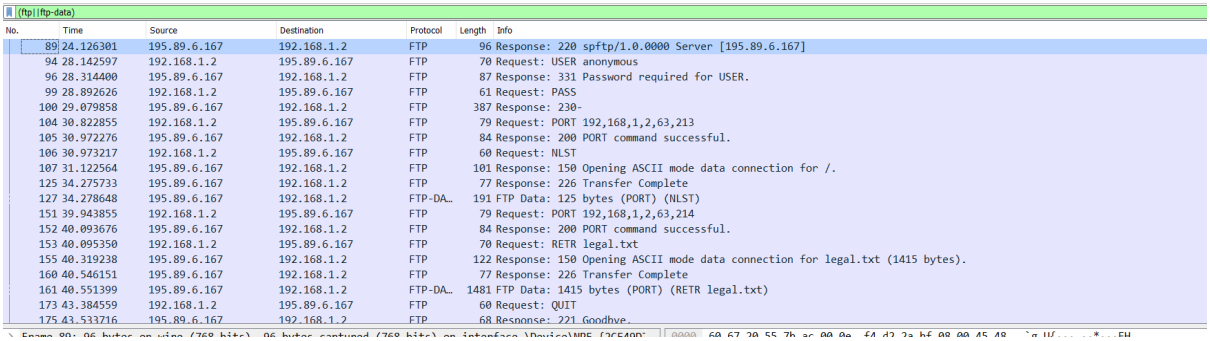
Question 1:

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



No.	Time	Source	Destination	Protocol	Length	Info
89	24.126301	195.89.6.167	192.168.1.2	FTP	96	Response: 220 spftp/1.0.0000 Server [195.89.6.167]
94	28.142597	192.168.1.2	195.89.6.167	FTP	70	Request: USER anonymous
96	28.314400	195.89.6.167	192.168.1.2	FTP	87	Response: 331 Password required for USER.
99	28.892626	192.168.1.2	195.89.6.167	FTP	61	Request: PASS
100	29.079858	195.89.6.167	192.168.1.2	FTP	387	Response: 230-
104	30.822855	192.168.1.2	195.89.6.167	FTP	79	Request: PORT 192,168,1,2,63,213
105	30.972276	195.89.6.167	192.168.1.2	FTP	84	Response: 200 PORT command successful.
106	30.973217	192.168.1.2	195.89.6.167	FTP	60	Request: NLST
107	31.122564	195.89.6.167	192.168.1.2	FTP	101	Response: 150 Opening ASCII mode data connection for /.
125	34.275733	195.89.6.167	192.168.1.2	FTP	77	Response: 226 Transfer Complete
127	34.278648	195.89.6.167	192.168.1.2	FTP-DA…	191	FTP Data: 125 bytes (PORT) (NLST)
151	39.943855	192.168.1.2	195.89.6.167	FTP	79	Request: PORT 192,168,1,2,63,214
152	40.093676	195.89.6.167	192.168.1.2	FTP	84	Response: 200 PORT command successful.
153	40.095350	192.168.1.2	195.89.6.167	FTP	70	Request: RETR legal.txt
155	40.319238	195.89.6.167	192.168.1.2	FTP	122	Response: 150 Opening ASCII mode data connection for legal.txt (1415 bytes).
160	40.546151	195.89.6.167	192.168.1.2	FTP	77	Response: 226 Transfer Complete
161	40.551399	195.89.6.167	192.168.1.2	FTP-DA…	1481	FTP Data: 1415 bytes (PORT) (RETR legal.txt)
173	43.384559	192.168.1.2	195.89.6.167	FTP	60	Request: QUIT
175	43.533716	195.89.6.167	192.168.1.2	FTP	68	Response: 221 Goodbye.

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?

	Time	Source	Destination	Protocol	Length	Info
36	0.690072	192.168.100.1	192.168.33.110	ICMP	90	Destination unreachable (Port unreachable)
37	0.690141	192.168.100.1	192.168.33.110	ICMP	90	Destination unreachable (Port unreachable)
41	0.921512	123.176.22.2	192.168.33.110	ICMP	90	Destination unreachable (Port unreachable)
48	1.475835	192.168.33.110	172.217.27.36	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, t
50	1.574198	172.217.27.36	192.168.33.110	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, t
56	1.688922	192.168.100.1	192.168.33.110	ICMP	90	Destination unreachable (Port unreachable)
77	2.476545	192.168.33.110	172.217.27.36	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, t
82	2.638204	172.217.27.36	192.168.33.110	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, t
88	2.667579	192.168.100.1	192.168.33.110	ICMP	173	Destination unreachable (Port unreachable)
101	3.477593	192.168.33.110	172.217.27.36	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, t
102	3.575973	172.217.27.36	192.168.33.110	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, t

They are not sent over TCP or UDP, they have their own protocol.

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

```
Ethernet II, Src: Tp-LinkT_87:05:fe (c0:4a:00:87:05:fe), Dst: IntelCor_55:7b:ac (60:67:20:55:7b:ac)
  Destination: IntelCor_55:7b:ac (60:67:20:55:7b:ac)
  Source: Tp-LinkT_87:05:fe (c0:4a:00:87:05:fe)
```

Source: Tp-LinkT_87:05:fe (c0:4a:00:87:05:fe)

Destination: IntelCor_55:7b:ac (60:67:20:55:7b:ac)

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

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

Type: 8 request which is used for ping requests

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	Destination	Protocol	L
	192.168.33.110	172.217.27.36	ICMP	
	172.217.27.36	192.168.33.110	ICMP	
	192.168.100.1	192.168.33.110	ICMP	
	192.168.33.110	172.217.27.36	ICMP	
	172.217.27.36	192.168.33.110	ICMP	
	192.168.100.1	192.168.33.110	ICMP	
	192.168.33.110	172.217.27.36	ICMP	
	172.217.27.36	192.168.33.110	ICMP	

The IP Address of the host is: 192.168.33.100

The IP Address of the Destination is: 172.217.27.36

6- 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.

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 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 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.

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d38 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 35 (0x0023)
    Sequence Number (LE): 8960 (0x2300)
    [Response frame: 82]
```

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.

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x5538 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 35 (0x0023)
    Sequence Number (LE): 8960 (0x2300)
    [Request frame: 77]
    [Response time: 161.659 ms]
```

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?

```
Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x3af7 [correct]
    [Checksum Status: Good]
    Unused: 00000000
```

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