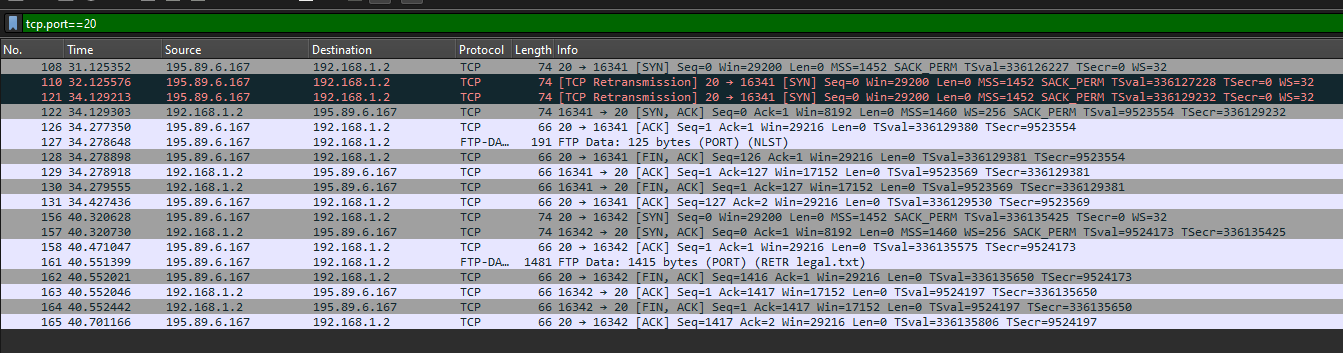
**Syed Farhan Jafri**

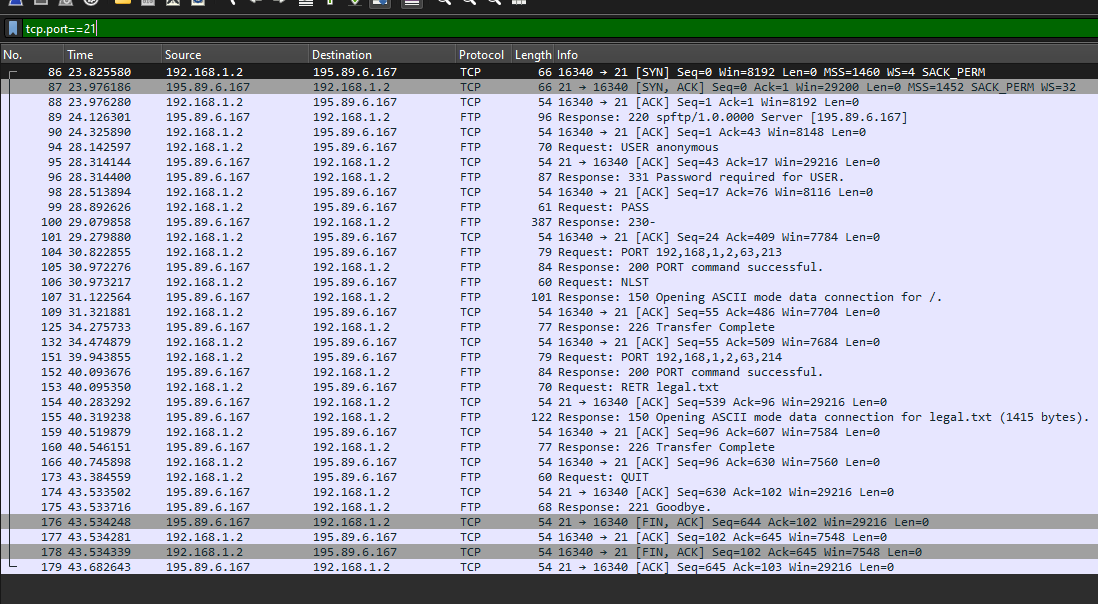
**21L-6074**

**BSE-6A2**

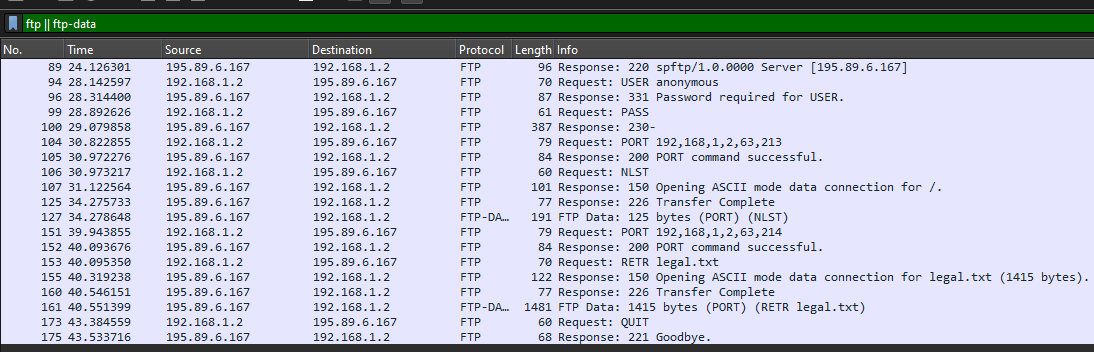
**CN Lab 4**

**Lab Statement 1**

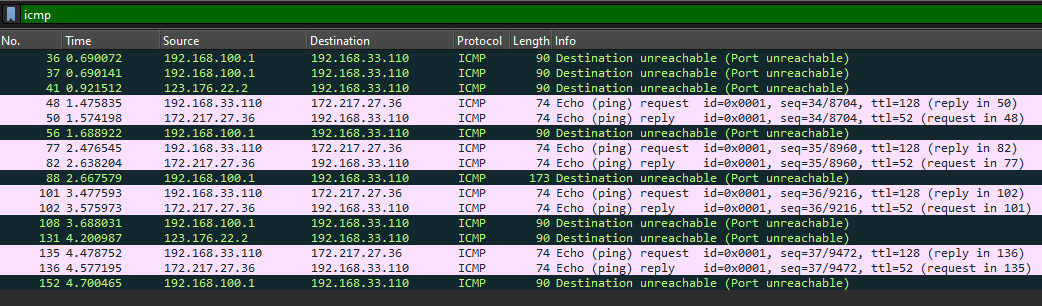
**1.**

**TCP Port 20 is the data channel. It is used to send the data files between the client and the server.**

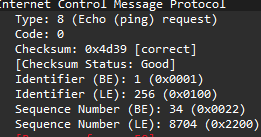
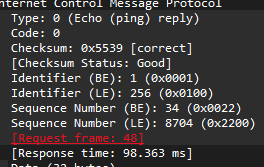
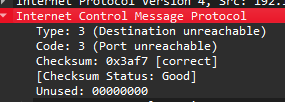
**TCP Port 21 is the control channel. It is used for passing control information.**

**2.**

1. **Packet 89:** FTP response from the server (with IP address 195.89.6.167) to the client (192.168.1.2), indicating that the server is ready.
2. **Packet 94:** FTP request from the client to the server, where the client is sending the "USER" command followed by "anonymous" to log in to the FTP server as an anonymous user.
3. **Packet 96:** FTP response from the server to the client, indicating that the username was accepted but a password is now required to complete the authentication process.
4. **Packet 99:** FTP request from the client to the server, where the client is sending the "PASS" command.
5. **Packet 100:** FTP response from the server to the client, where the response code "230" indicates successful authentication.
6. **Packet 104:** Client asks server to send the data on IP:192.168.1.2 and Port:16341
7. **Packet 105:** Server acknowledges the client's request to establish a data connection on the specified port and is ready to use this port for data transfer operations.
8. **Packet 106:** Client is requesting a list of files and directories in the current directory on the server.
9. **Packet 107:** Server is opening a data connection in ASCII mode to transfer the list of files and directories.
10. **Packet 125:** The packet is indicating that the data transfer has been successfully completed.
11. **Packet 127:** This packet, labeled as "FTP-DATA," represents the actual data transfer between the FTP server and the client over the data connection established. The packet contains 125 bytes of data
12. **Packet 151:** The client is using the "PORT" command again to specify a new address and port number for a subsequent data connection. The IP address remains the client's IP (192,168,1,2), and the new port bytes "63,214" translate to a slightly different port number.
13. **Packet 152:** The new PORT command sent by the client has been successfully processed.
14. **Packet 153:** The client is using the "RETR" command followed by "legal.txt" to request the download of a file named "legal.txt" from the server. The "RETR" command is used to retrieve or download files from the FTP server to the client.
15. **Packet 155:** Server is opening a data connection in ASCII mode to transfer the file "legal.txt". The file size is 1415 bytes.
16. **Packet 160:** File transfer has been successfully completed.
17. **Packet 161:** This packet, marked as "FTP-DATA," represents the actual data transfer from the FTP server to the client. The packet contains 1415 bytes of data.
18. **Packet 173:** Client is sending the "QUIT" command to close the FTP session.
19. **Packet 175:** Server has acknowledged the client's "QUIT" command and is closing the control connection.

**Lab Statement 2**

1. ICMP messages are not sent over UDP oor TCP. ICMP operates at the network layer. It is encapsulated within IP datagrams, making it independent of TCP and UDP, which operate at the transport layer.
2. **Ethernet Address of Host**: Dst: TpLinkTechno\_87:05:fe (c0:4a:00:87:05:fe)
3. Echo (ping) request is sent through these ICMP packets. These are used to test the reachability of a host on an IP network.
4. **4** Echo (ping) requests are sent through the host. Packet 48, 77, 101, 135.
5. **IP address of your host:** 192.168.33.110.   
   **IP address of the destination host:** 172.217.27.36
6. An ICMP packet does not have source and destination port numbers because it is not encapsulated within TCP or UDP segments. ICMP operates at the network layer, directly within IP packets, and does not use port numbers.
7. The values that differentiate an ICMP request message from an ICMP reply message include the ICMP type field.   
   Echo Request: 8  
   Echo Reply: 0

1. **For Packet 48:  
   ICMP Type:** 8 **ICMP Code Number:** 0  **Checksum:** 2bytes **Sequence Number:** 2bytes **Identifier Fields:** 2bytes
2. **For Packet 49:  
   ICMP Type:** 0 **ICMP Code Number:** 0  **Checksum:** 2bytes **Sequence Number:** 2bytes **Identifier Fields:** 2bytes  
   **Response Time:** 98.363ms **Request Frame:** 48
3. **For Packet 56:  
   ICMP Type:** 3 **ICMP Code Number:** 3The IP and TCP headers are included in the ICMP message to provide the sender with enough context to understand which packet caused the problem.

These headers show the original packet that triggered the unreachable message, including source and destination IP addresses helping the sender find the issue.