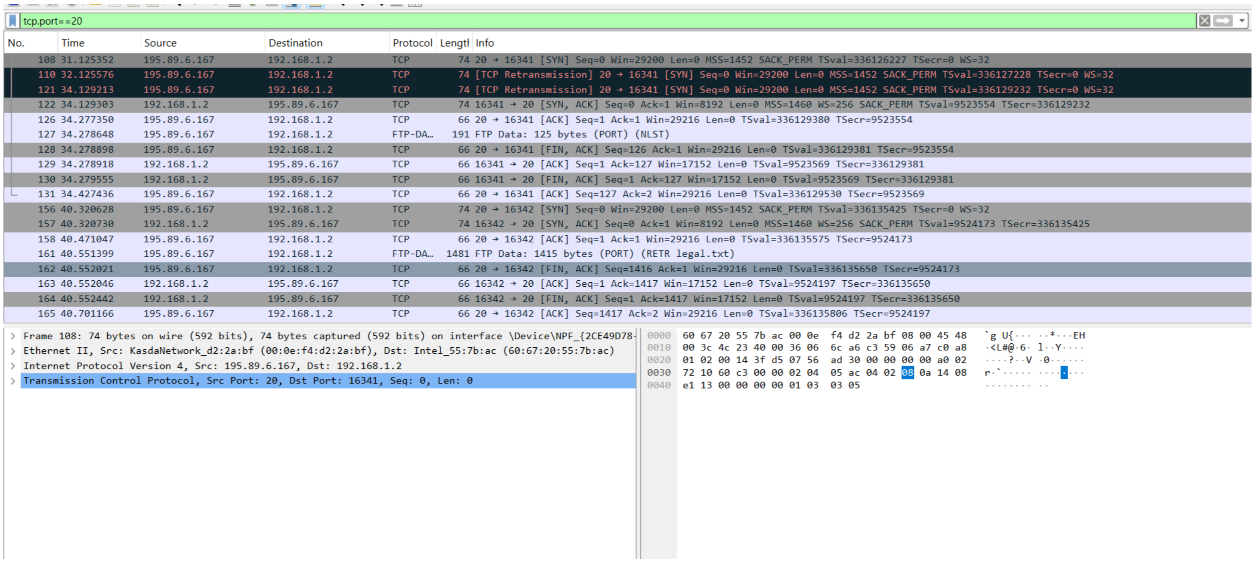
Hasan Yahya (22L-7971) - (BSE-6C)

Lab Statement: 01

1)

tcp.port==20



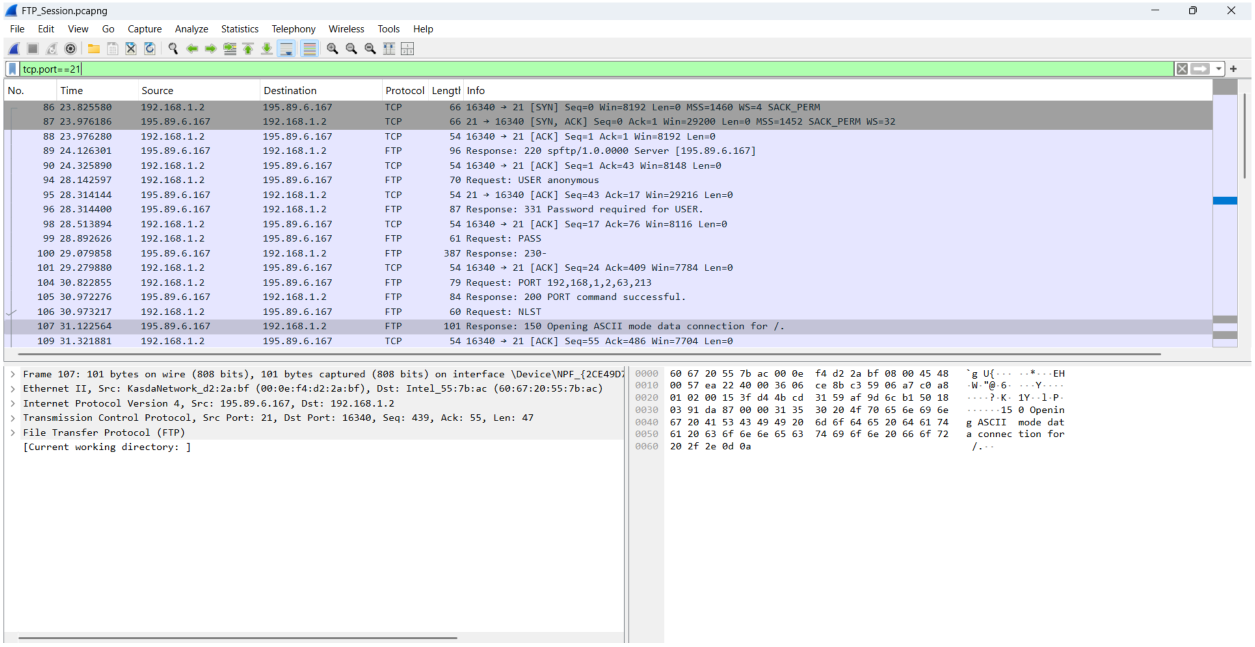
```
tcp.port==20
```

```
No.   Time        Source         Destination    Protocol  Lengtl Info
  108 31.125352   195.89.6.167   192.168.1.2    TCP         74 20 → 16341 [SYN] Seq=0 Win=29200 Len=0 MSS=1452 SACK_PERM TSval=336126227 TSecr=0 WS=32
  110 32.125576   195.89.6.167   192.168.1.2    TCP         74 [TCP Retransmission] 20 → 16341 [SYN] Seq=0 Win=29200 Len=0 MSS=1452 SACK_PERM TSval=336127228 TSecr=0 WS=32
  121 34.129213   195.89.6.167   192.168.1.2    TCP         74 [TCP Retransmission] 20 → 16341 [SYN] Seq=0 Win=29200 Len=0 MSS=1452 SACK_PERM TSval=336129232 TSecr=0 WS=32
  122 34.129303   192.168.1.2    195.89.6.167   TCP         74 16341 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=9523554 TSecr=336129232
  126 34.277350   195.89.6.167   192.168.1.2    TCP         66 20 → 16341 [ACK] Seq=1 Ack=1 Win=29216 Len=0 TSval=336129380 TSecr=9523554
  127 34.278648   195.89.6.167   192.168.1.2    FTP-DA…    191 FTP Data: 125 bytes (PORT) (NLST)
  128 34.278898   195.89.6.167   192.168.1.2    TCP         66 20 → 16341 [FIN, ACK] Seq=126 Ack=1 Win=29216 Len=0 TSval=336129381 TSecr=9523554
  129 34.278918   192.168.1.2    195.89.6.167   TCP         66 16341 → 20 [ACK] Seq=1 Ack=127 Win=17152 Len=0 TSval=9523569 TSecr=336129381
  130 34.279555   192.168.1.2    195.89.6.167   TCP         66 16341 → 20 [FIN, ACK] Seq=1 Ack=127 Win=17152 Len=0 TSval=9523569 TSecr=336129381
  131 34.427436   195.89.6.167   192.168.1.2    TCP         66 20 → 16341 [ACK] Seq=127 Ack=2 Win=29216 Len=0 TSval=336129530 TSecr=9523569
  156 40.320628   195.89.6.167   192.168.1.2    TCP         74 20 → 16342 [SYN] Seq=0 Win=29200 Len=0 MSS=1452 SACK_PERM TSval=336135425 TSecr=0 WS=32
  157 40.320730   192.168.1.2    195.89.6.167   TCP         74 16342 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=9524173 TSecr=336135425
  158 40.471047   195.89.6.167   192.168.1.2    TCP         66 20 → 16342 [ACK] Seq=1 Ack=1 Win=29216 Len=0 TSval=336135575 TSecr=9524173
  161 40.551399   195.89.6.167   192.168.1.2    FTP-DA…   1481 FTP Data: 1415 bytes (PORT) (RETR legal.txt)
  162 40.552021   195.89.6.167   192.168.1.2    TCP         66 20 → 16342 [FIN, ACK] Seq=1416 Ack=1 Win=29216 Len=0 TSval=336135650 TSecr=9524173
  163 40.552046   192.168.1.2    195.89.6.167   TCP         66 16342 → 20 [ACK] Seq=1 Ack=1417 Win=17152 Len=0 TSval=9524197 TSecr=336135650
  164 40.552442   192.168.1.2    195.89.6.167   TCP         66 16342 → 20 [FIN, ACK] Seq=1 Ack=1417 Win=17152 Len=0 TSval=9524197 TSecr=336135650
  165 40.701166   195.89.6.167   192.168.1.2    TCP         66 20 → 16342 [ACK] Seq=1417 Ack=2 Win=29216 Len=0 TSval=336135806 TSecr=9524197
```

```
> Frame 108: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2CE49D78-
> Ethernet II, Src: KasdaNetwork_d2:2a:bf (00:0e:f4:d2:2a:bf), Dst: Intel_55:7b:ac (60:67:20:55:7b:ac)
> Internet Protocol Version 4, Src: 195.89.6.167, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 20, Dst Port: 16341, Seq: 0, Len: 0
```

```
0000  60 67 20 55 7b ac 00 0e  f4 d2 2a bf 08 00 45 48   `g U{··· ··*···EH
0010  00 3c 4c 23 40 00 36 06  6c a6 c3 59 06 a7 c0 a8   ·<L#@·6· l··Y····
0020  01 02 00 14 3f d5 07 56  ad 30 00 00 00 00 a0 02   ····?··V ·0······
0030  72 10 60 c3 00 00 02 04  05 ac 04 02 08 0a 14 08   r·`····· ········
0040  e1 13 00 00 00 00 01 03  03 05                     ········ ··
```

tcp.port==21

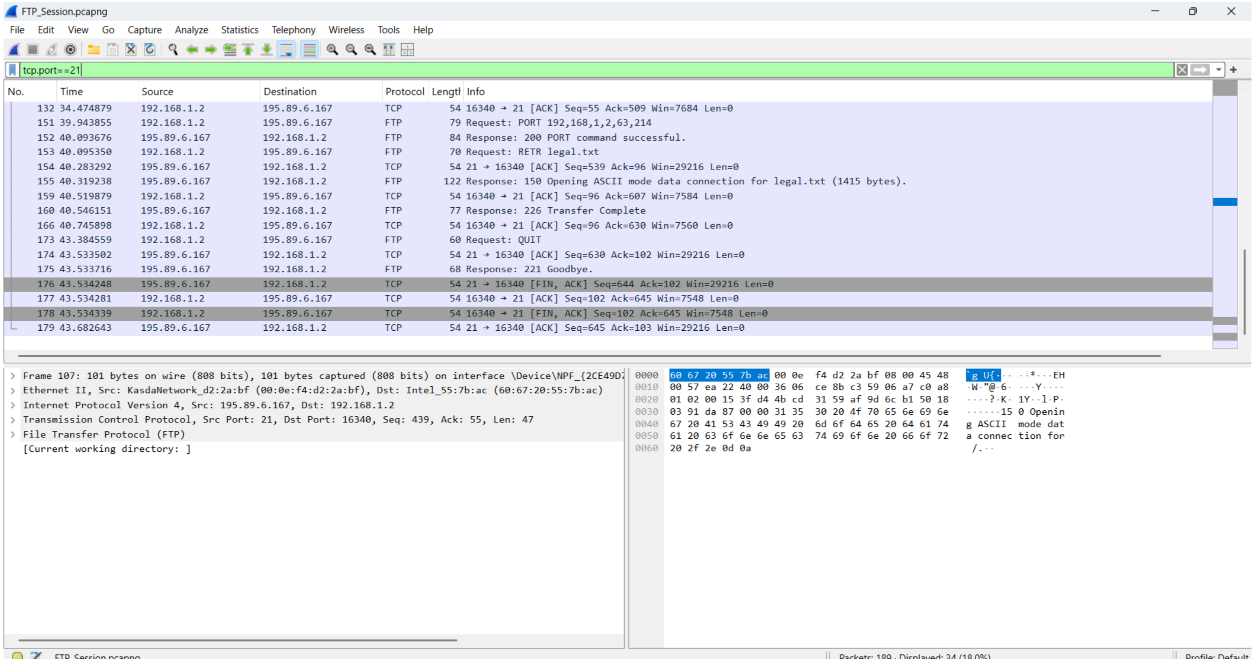


```
tcp.port==21
```

```
No.   Time        Source         Destination    Protocol Lengtl Info
   86 23.825580   192.168.1.2    195.89.6.167   TCP        66 16340 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
   87 23.976186   195.89.6.167   192.168.1.2    TCP        66 21 → 16340 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=32
   88 23.976280   192.168.1.2    195.89.6.167   TCP        54 16340 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0
   89 24.126301   195.89.6.167   192.168.1.2    FTP        96 Response: 220 spftp/1.0.0000 Server [195.89.6.167]
   90 24.325890   192.168.1.2    195.89.6.167   TCP        54 16340 → 21 [ACK] Seq=1 Ack=43 Win=8148 Len=0
   94 28.142597   192.168.1.2    195.89.6.167   FTP        70 Request: USER anonymous
   95 28.314144   195.89.6.167   192.168.1.2    TCP        54 21 → 16340 [ACK] Seq=43 Ack=17 Win=29216 Len=0
   96 28.314400   195.89.6.167   192.168.1.2    FTP        87 Response: 331 Password required for USER.
   98 28.513894   192.168.1.2    195.89.6.167   TCP        54 16340 → 21 [ACK] Seq=17 Ack=76 Win=8116 Len=0
   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-
  101 29.279880   192.168.1.2    195.89.6.167   TCP        54 16340 → 21 [ACK] Seq=24 Ack=409 Win=7784 Len=0
  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 /.
  109 31.321881   192.168.1.2    195.89.6.167   TCP        54 16340 → 21 [ACK] Seq=55 Ack=486 Win=7704 Len=0
```

```
> Frame 107: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{2CE49D7
> Ethernet II, Src: KasdaNetwork_d2:2a:bf (00:0e:f4:d2:2a:bf), Dst: Intel_55:7b:ac (60:67:20:55:7b:ac)
> Internet Protocol Version 4, Src: 195.89.6.167, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 16340, Seq: 439, Ack: 55, Len: 47
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  60 67 20 55 7b ac 00 0e  f4 d2 2a bf 08 00 45 48   `g U{··· ··*···EH
0010  00 57 ea 22 40 00 36 06  ce 8b c3 59 06 a7 c0 a8   ·W·"@·6· ···Y····
0020  01 02 00 15 3f d4 4b cd  31 59 af 9d 6c b1 50 18   ····?·K· 1Y··l·P·
0030  03 91 da 87 00 00 31 35  30 20 4f 70 65 6e 69 6e   ······15 0 Openin
0040  67 20 41 53 43 49 49 20  6d 6f 64 65 20 64 61 74   g ASCII  mode dat
0050  61 20 63 6f 6e 6e 65 63  74 69 6f 6e 20 66 6f 72   a connec tion for
0060  20 2f 2e 0d 0a                                      /.··
```


FTP_Session.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==21
```

```
No.   Time       Source        Destination   Protocol Lengtl Info
  132 34.474879  192.168.1.2   195.89.6.167  TCP       54 16340 → 21 [ACK] Seq=55 Ack=509 Win=7684 Len=0
  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
  154 40.283292  195.89.6.167  192.168.1.2   TCP       54 21 → 16340 [ACK] Seq=539 Ack=96 Win=29216 Len=0
  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).
  159 40.519879  192.168.1.2   195.89.6.167  TCP       54 16340 → 21 [ACK] Seq=96 Ack=607 Win=7584 Len=0
  160 40.546151  195.89.6.167  192.168.1.2   FTP       77 Response: 226 Transfer Complete
  166 40.745898  192.168.1.2   195.89.6.167  TCP       54 16340 → 21 [ACK] Seq=96 Ack=630 Win=7560 Len=0
  173 43.384559  192.168.1.2   195.89.6.167  FTP       60 Request: QUIT
  174 43.533502  195.89.6.167  192.168.1.2   TCP       54 21 → 16340 [ACK] Seq=630 Ack=102 Win=29216 Len=0
  175 43.533716  195.89.6.167  192.168.1.2   FTP       68 Response: 221 Goodbye.
  176 43.534248  195.89.6.167  192.168.1.2   TCP       54 21 → 16340 [FIN, ACK] Seq=644 Ack=102 Win=29216 Len=0
  177 43.534281  192.168.1.2   195.89.6.167  TCP       54 16340 → 21 [ACK] Seq=102 Ack=645 Win=7548 Len=0
  178 43.534339  192.168.1.2   195.89.6.167  TCP       54 16340 → 21 [FIN, ACK] Seq=102 Ack=645 Win=7548 Len=0
  179 43.682643  195.89.6.167  192.168.1.2   TCP       54 21 → 16340 [ACK] Seq=645 Ack=103 Win=29216 Len=0
```

```
> Frame 107: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface \Device\NPF_{2CE49D7
> Ethernet II, Src: KasdaNetwork_d2:2a:bf (00:0e:f4:d2:2a:bf), Dst: Intel_55:7b:ac (60:67:20:55:7b:ac)
> Internet Protocol Version 4, Src: 195.89.6.167, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 16340, Seq: 439, Ack: 55, Len: 47
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

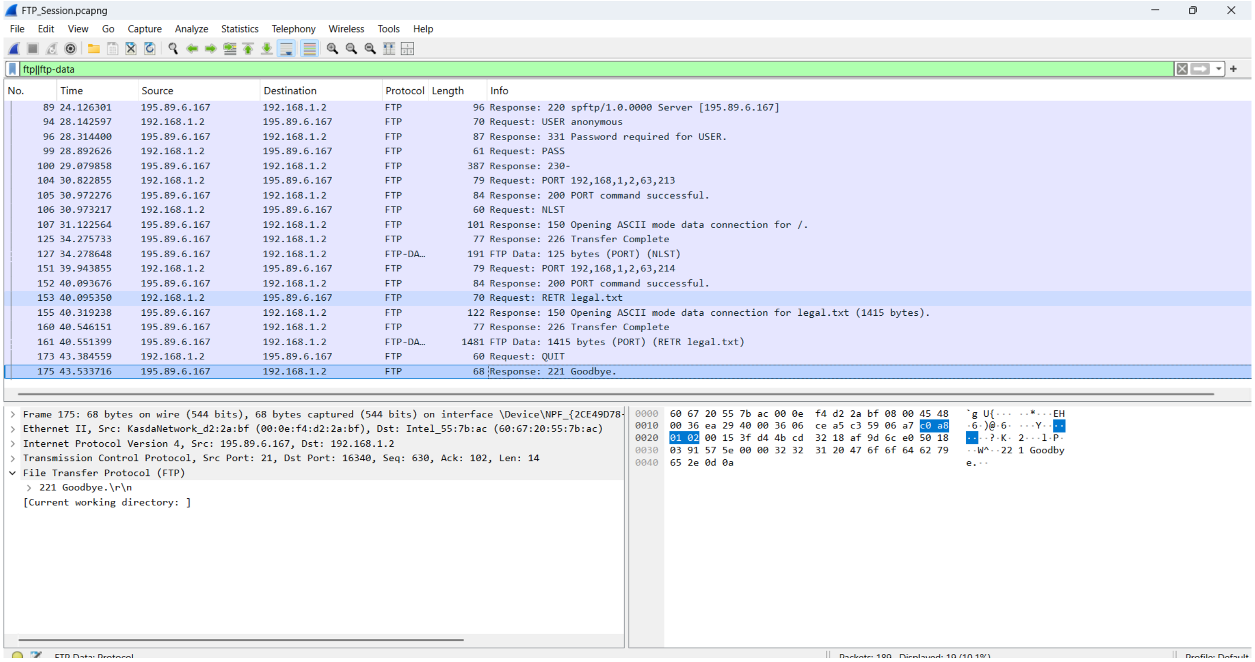
```
0000  60 67 20 55 7b ac 00 0e  f4 d2 2a bf 08 00 45 48   `g U{··· ··*···EH
0010  00 57 ea 22 40 00 36 06  ce 8b c3 59 06 a7 c0 a8   ·W·"@·6· ···Y····
0020  01 02 00 15 3f d4 4b cd  31 59 af 9d 6c b1 50 18   ····?·K· 1Y··l·P·
0030  03 91 da 87 00 00 31 35  30 20 4f 70 65 6e 69 6e   ······15 0 Openin
0040  67 20 41 53 43 49 49 20  6d 6f 64 65 20 64 61 74   g ASCII  mode dat
0050  61 20 63 6f 6e 6e 65 63  74 69 6f 6e 20 66 6f 72   a connec tion for
0060  20 2f 2e 0d 0a                                      /.··
```

Port 21 (Control Connection): This is used for sending FTP commands and receiving responses.
Port 20 (Data Connection): This is used for actual file transfer when in Active Mode.

2)

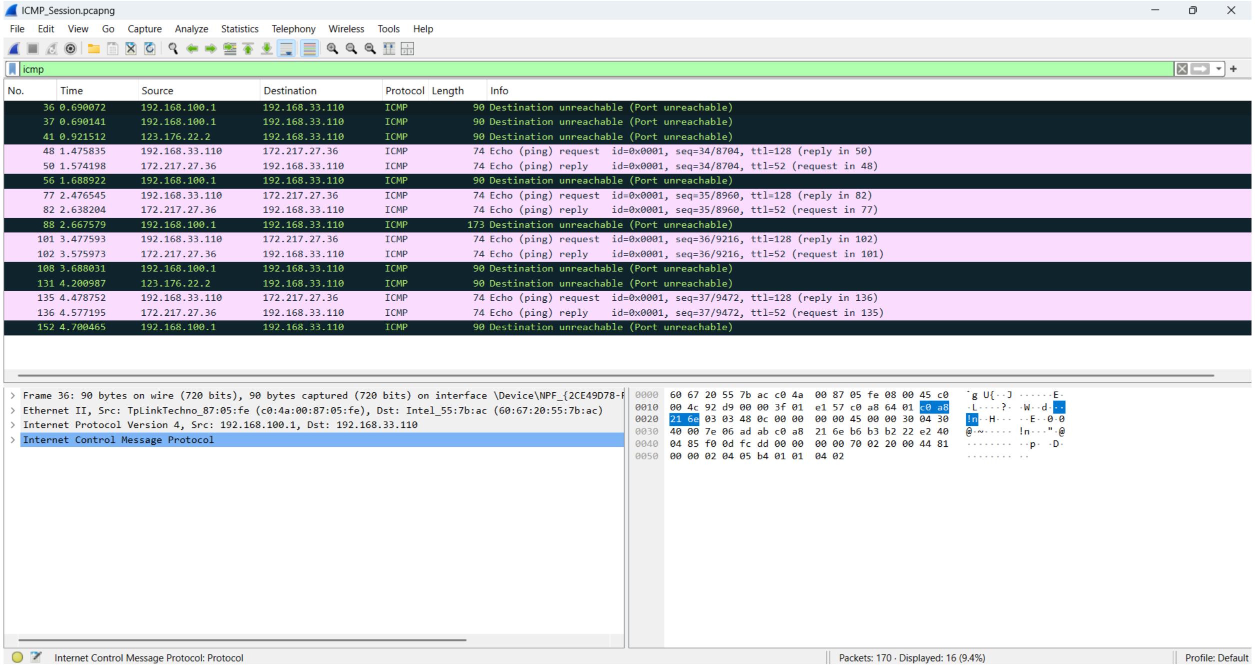
Packet no:	Details:
89	Server (195.89.6.167) greets the client with an FTP “220” message, indicating it is ready to accept connections.
94	Client (192.168.1.2) sends the USER anonymous command to log in as an anonymous user.
96	Server (195.89.6.167) replies with “331,” asking the client to provide a password for the anonymous login.
99	Client (192.168.1.2) issues the PASS command, supplying the password for the anonymous account.
100	Server (195.89.6.167) indicates successful authentication (“230”), confirming the client is now logged in.
104	The client (192.168.1.2) is requesting the FTP server (195.89.6.167) to establish an active mode data connection to IP 192.168.1.2 on port 16281. As (63×256)+213=16281
105	The FTP server (195.89.6.167) acknowledges the client's PORT command

	from Packet 104, confirming that it will use the specified IP (192.168.1.2) and port (16281) for the upcoming data transfer.
106	The client (192.168.1.2) requests a list of filenames in the current directory from the FTP server (195.89.6.167). The NLST (Name List) command is similar to LIST, but it only returns filenames without additional details like file sizes or permissions.
107	The FTP server (195.89.6.167) informs the client (192.168.1.2) that it is about to send the directory listing in ASCII mode over the data connection previously established on port 16281. This response indicates that the server is preparing to transfer the requested NLST data.
125	The FTP server (195.89.6.167) confirms that the directory listing transfer requested by the client (192.168.1.2) using the NLST command has been successfully completed. The server has finished sending the list of filenames over the data connection.
127	The FTP server (195.89.6.167) sends 125 bytes of directory listing data to the client (192.168.1.2) in response to the NLST command. This data contains the list of filenames from the requested directory, transferred over the previously established data connection (PORT mode).
151	The client (192.168.1.2) requests the FTP server (195.89.6.167) to establish a new active mode data connection. The client specifies its IP (192.168.1.2) and port 16270 for the upcoming data transfer.
152	The FTP server (195.89.6.167) acknowledges the client's PORT command from Packet 152, confirming that it will use the specified IP (192.168.1.2) and port 16270 for the upcoming data transfer.
153	The client (192.168.1.2) requests to retrieve (download) the file named legal.txt from the FTP server (195.89.6.167).
155	The FTP server (195.89.6.167) confirms that it is starting the file transfer of legal.txt (size: 1415 bytes) to the client (192.168.1.2) in ASCII mode.
160	The FTP server (195.89.6.167) confirms that the requested file legal.txt has been successfully transferred to the client (192.168.1.2).
161	The FTP server (195.89.6.167) sends 1415 bytes of file data to the client (192.168.1.2) as part of the file transfer request (RETR legal.txt).
173	The client (192.168.1.2) sends the QUIT command to gracefully terminate the FTP session with the server (195.89.6.167). This signals the end of the session, and the server will respond accordingly.
175	The FTP server (195.89.6.167) acknowledges the client's QUIT command from Packet 173, confirming that the session is being closed. The control connection between the client and the server is now terminated.


FTP_Session.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ftp||ftp-data

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.

> Frame 175: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{2CE49D78-
> Ethernet II, Src: KasdaNetwork_d2:2a:bf (00:0e:f4:d2:2a:bf), Dst: Intel_55:7b:ac (60:67:20:55:7b:ac)
> Internet Protocol Version 4, Src: 195.89.6.167, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 16340, Seq: 630, Ack: 102, Len: 14
v File Transfer Protocol (FTP)
  > 221 Goodbye.\r\n
  [Current working directory: ]

0000  60 67 20 55 7b ac 00 0e  f4 d2 2a bf 08 00 45 48   `g U{··· ··*···EH
0010  00 36 ea 29 40 00 36 06  ce a5 c3 59 06 a7 c0 a8   ·6·)@·6· ···Y····
0020  01 02 00 15 3f d4 4b cd  32 18 af 9d 6c e0 50 18   ····?·K· 2···l·P·
0030  03 91 57 5e 00 00 32 32  31 20 47 6f 6f 64 62 79   ··W^··22 1 Goodby
0040  65 2e 0d 0a                                        e.··

FTP Data: Protocol    Packets: 189 · Displayed: 19 (10.1%)    Profile: Default
```

Lab Statement: 03

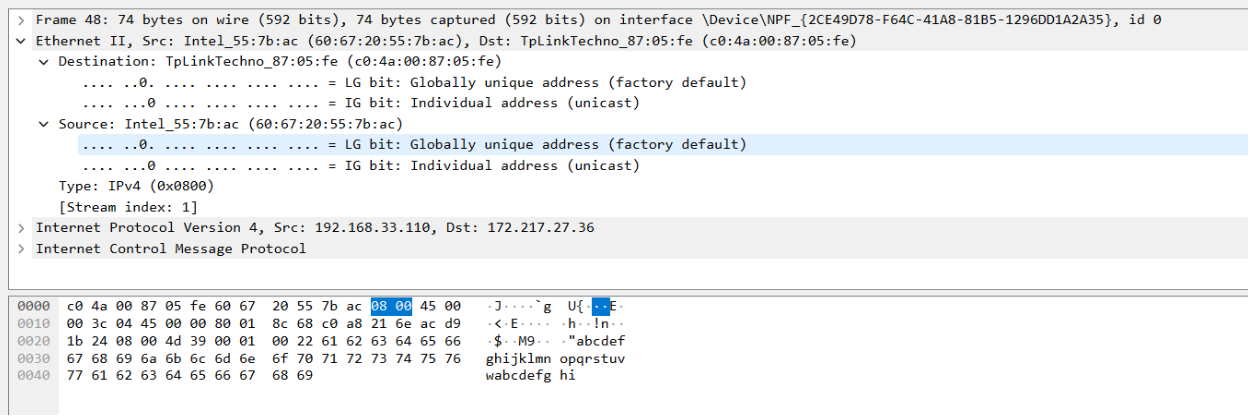

ICMP_Session.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp

No.  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, ttl=128 (reply in 50)
  50 1.574198 172.217.27.36   192.168.33.110  ICMP         74 Echo (ping) reply    id=0x0001, seq=34/8704, ttl=52 (request in 48)
  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, ttl=128 (reply in 82)
  82 2.638204 172.217.27.36   192.168.33.110  ICMP         74 Echo (ping) reply    id=0x0001, seq=35/8960, ttl=52 (request in 77)
  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, ttl=128 (reply in 102)
 102 3.575973 172.217.27.36   192.168.33.110  ICMP         74 Echo (ping) reply    id=0x0001, seq=36/9216, ttl=52 (request in 101)
 108 3.688031 192.168.100.1   192.168.33.110  ICMP         90 Destination unreachable (Port unreachable)
 131 4.200987 123.176.22.2    192.168.33.110  ICMP         90 Destination unreachable (Port unreachable)
 135 4.478752 192.168.33.110  172.217.27.36   ICMP         74 Echo (ping) request  id=0x0001, seq=37/9472, ttl=128 (reply in 136)
 136 4.577195 172.217.27.36   192.168.33.110  ICMP         74 Echo (ping) reply    id=0x0001, seq=37/9472, ttl=52 (request in 135)
 152 4.700465 192.168.100.1   192.168.33.110  ICMP         90 Destination unreachable (Port unreachable)

> Frame 36: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{2CE49D78-F
> Ethernet II, Src: TpLinkTechno_87:05:fe (c0:4a:00:87:05:fe), Dst: Intel_55:7b:ac (60:67:20:55:7b:ac)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 192.168.33.110
> Internet Control Message Protocol

0000  60 67 20 55 7b ac c0 4a  00 87 05 fe 08 00 45 c0   `g U{··J ······E·
0010  00 4c 92 d9 00 00 3f 01  e1 57 c0 a8 64 01 c0 a8   ·L····?· ·W··d···
0020  21 6e 03 03 48 0c 00 00  00 00 45 00 00 30 04 30   !n··H··· ··E··0·0
0030  40 00 7e 06 ad ab c0 a8  21 6e b6 b3 b2 22 e2 40   @·~····· !n···"·@
0040  04 85 f0 0d fc dd 00 00  00 00 70 02 20 00 44 81   ········ ··p· ·D·
0050  00 00 02 04 05 b4 01 01  04 02                     ········ ··

Internet Control Message Protocol: Protocol    Packets: 170 · Displayed: 16 (9.4%)    Profile: Default
```

1)

ICMP does not run on top of UDP or TCP. It is encapsulated directly in IP (protocol number 1 in the IP header).

2)



```
> Frame 48: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2CE49D78-F64C-41A8-81B5-1296DD1A2A35}, id 0
v Ethernet II, Src: Intel_55:7b:ac (60:67:20:55:7b:ac), Dst: TpLinkTechno_87:05:fe (c0:4a:00:87:05:fe)
  v Destination: TpLinkTechno_87:05:fe (c0:4a:00:87:05:fe)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Intel_55:7b:ac (60:67:20:55:7b:ac)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Internet Protocol Version 4, Src: 192.168.33.110, Dst: 172.217.27.36
> Internet Control Message Protocol

0000  c0 4a 00 87 05 fe 60 67  20 55 7b ac 08 00 45 00   ·J····`g U{···E·
0010  00 3c 04 45 00 00 80 01  8c 68 c0 a8 21 6e ac d9   ·<·E···· ·h··!n··
0020  1b 24 08 00 4d 39 00 01  00 22 61 62 63 64 65 66   ·$··M9·· ·"abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Address for source host is 60:67:20:55:7b:ac (MAC Address)
Address for destination host is c0:4a:00:87:05:fe (MAC Address)

3)

They are ICMP Echo Request messages, commonly known as “ping” requests.

4)

4 requests are sent through host

5)

Source host is 192.168.33.110
Destination host is 172.217.27.26

6)

ICMP operates at the network layer (layer 3) rather than the transport layer. Ports (source port, destination port) are a concept of transport-layer protocols (like TCP or UDP). ICMP, by contrast, is identified by its type and code fields and does not use ports.

7)

The type field, for request it is 8 and for response it is 0.

8)

ICMP type and code: For a request, typically Type = 8, Code = 0.
Checksum (2 bytes)
Identifier (2 bytes)
Sequence Number (2 bytes)
Data (variable length, often some ASCII data to pad out the packet)

9)

For a reply, typically Type = 0, Code = 0.
Checksum (2 bytes)
Identifier (2 bytes, same as request)
Sequence Number (2 bytes, same as request)
Data (variable length, mirrors what was sent is request)

10)

“Destination Unreachable” is Type = 3
“Port Unreachable” is Code = 3
ICMP error messages (such as destination unreachable) include: The original IP header, the first 8 (or more) bytes of the original transport-layer header (TCP/UDP). This is done so the sender can identify which socket/connection or which packet triggered the error, so that we know what part of the network caused the error.

These headers depict the offending packet, i.e., the packet that caused the “destination unreachable” error. By looking at that embedded IP + TCP header, the sender knows exactly which flow or port was unreachable.