Lab1 - Intro to Wireshark

Jiaxi Zhang

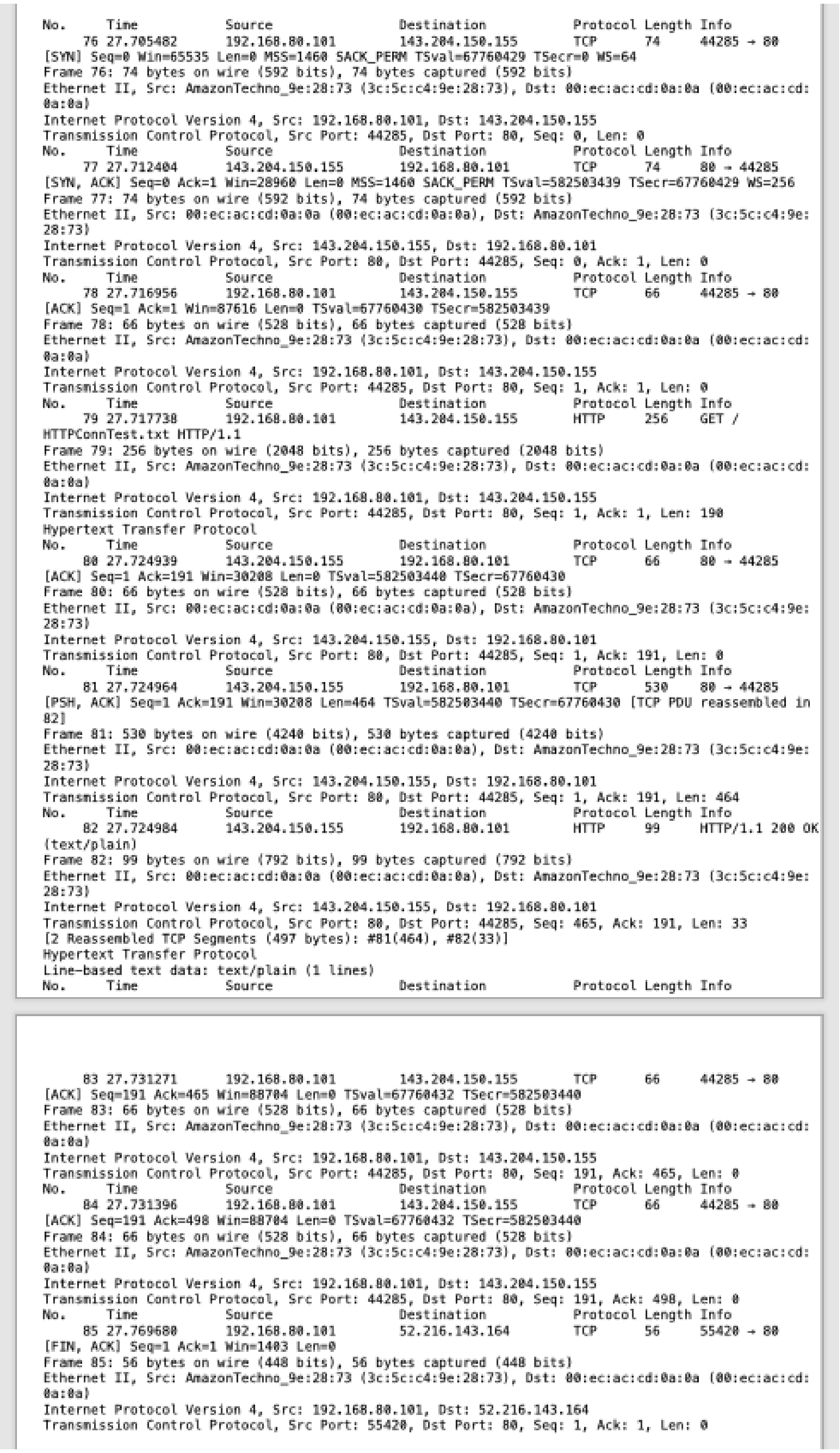
February 8, 2025

1 Three Different Protocols

- **HTTP** : Hypertext Transfer Protocol. It is from the application layer of the OSI model. It is used to transfer hypertext and display it on the web browser between the client and the server.
- **ARP** : Address Resolution Protocol. It is from the link layer of the OSI model. It is used to map an IP address to a MAC address so that the data can be correctly transmitted in LAN.
- **TCP** : Transmission Control Protocol. It is from the transport layer of the OSI model. It is used to establish a reliable data transmission between two hosts.

2 Analysis for Packets 76-85

The application protocol used in the packets 76-85 is HTTP which can be seen in packet 79 and 82 in the Protocol column, and in the Info column, we can see the GET request in 79 and the HTTP/1.1 200 OK response in 82. The total time for the request and response is 0.007246 seconds, which can be computed by the time difference between packet 79 and 82 (27.724984 - 27.717738 = 0.007246 seconds). The screenshot of the third question is shown below.



```
No.     Time           Source                Destination           Protocol Length Info
     76 27.705482      192.168.80.101        143.204.150.155       TCP      74     44285 → 80
[SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=67760429 TSecr=0 WS=64
Frame 76: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: AmazonTechno_9e:28:73 (3c:5c:c4:9e:28:73), Dst: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:
0a:0a)
Internet Protocol Version 4, Src: 192.168.80.101, Dst: 143.204.150.155
Transmission Control Protocol, Src Port: 44285, Dst Port: 80, Seq: 0, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     77 27.712404      143.204.150.155       192.168.80.101        TCP      74     80 → 44285
[SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=582503439 TSecr=67760429 WS=256
Frame 77: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:0a:0a), Dst: AmazonTechno_9e:28:73 (3c:5c:c4:9e:
28:73)
Internet Protocol Version 4, Src: 143.204.150.155, Dst: 192.168.80.101
Transmission Control Protocol, Src Port: 80, Dst Port: 44285, Seq: 0, Ack: 1, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     78 27.716956      192.168.80.101        143.204.150.155       TCP      66     44285 → 80
[ACK] Seq=1 Ack=1 Win=87616 Len=0 TSval=67760430 TSecr=582503439
Frame 78: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: AmazonTechno_9e:28:73 (3c:5c:c4:9e:28:73), Dst: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:
0a:0a)
Internet Protocol Version 4, Src: 192.168.80.101, Dst: 143.204.150.155
Transmission Control Protocol, Src Port: 44285, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     79 27.717738      192.168.80.101        143.204.150.155       HTTP     256    GET /
HTTPConnTest.txt HTTP/1.1
Frame 79: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
Ethernet II, Src: AmazonTechno_9e:28:73 (3c:5c:c4:9e:28:73), Dst: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:
0a:0a)
Internet Protocol Version 4, Src: 192.168.80.101, Dst: 143.204.150.155
Transmission Control Protocol, Src Port: 44285, Dst Port: 80, Seq: 1, Ack: 1, Len: 190
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
     80 27.724939      143.204.150.155       192.168.80.101        TCP      66     80 → 44285
[ACK] Seq=1 Ack=191 Win=30208 Len=0 TSval=582503440 TSecr=67760430
Frame 80: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:0a:0a), Dst: AmazonTechno_9e:28:73 (3c:5c:c4:9e:
28:73)
Internet Protocol Version 4, Src: 143.204.150.155, Dst: 192.168.80.101
Transmission Control Protocol, Src Port: 80, Dst Port: 44285, Seq: 1, Ack: 191, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     81 27.724964      143.204.150.155       192.168.80.101        TCP      530    80 → 44285
[PSH, ACK] Seq=1 Ack=191 Win=30208 Len=464 TSval=582503440 TSecr=67760430 [TCP PDU reassembled in
82]
Frame 81: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits)
Ethernet II, Src: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:0a:0a), Dst: AmazonTechno_9e:28:73 (3c:5c:c4:9e:
28:73)
Internet Protocol Version 4, Src: 143.204.150.155, Dst: 192.168.80.101
Transmission Control Protocol, Src Port: 80, Dst Port: 44285, Seq: 1, Ack: 191, Len: 464
No.     Time           Source                Destination           Protocol Length Info
     82 27.724984      143.204.150.155       192.168.80.101        HTTP     99     HTTP/1.1 200 OK
(text/plain)
Frame 82: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
Ethernet II, Src: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:0a:0a), Dst: AmazonTechno_9e:28:73 (3c:5c:c4:9e:
28:73)
Internet Protocol Version 4, Src: 143.204.150.155, Dst: 192.168.80.101
Transmission Control Protocol, Src Port: 80, Dst Port: 44285, Seq: 465, Ack: 191, Len: 33
[2 Reassembled TCP Segments (497 bytes): #81(464), #82(33)]
Hypertext Transfer Protocol
Line-based text data: text/plain (1 lines)
No.     Time           Source                Destination           Protocol Length Info
```

```
     83 27.731271      192.168.80.101        143.204.150.155       TCP      66     44285 → 80
[ACK] Seq=191 Ack=465 Win=88704 Len=0 TSval=67760432 TSecr=582503440
Frame 83: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: AmazonTechno_9e:28:73 (3c:5c:c4:9e:28:73), Dst: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:
0a:0a)
Internet Protocol Version 4, Src: 192.168.80.101, Dst: 143.204.150.155
Transmission Control Protocol, Src Port: 44285, Dst Port: 80, Seq: 191, Ack: 465, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     84 27.731396      192.168.80.101        143.204.150.155       TCP      66     44285 → 80
[ACK] Seq=191 Ack=498 Win=88704 Len=0 TSval=67760432 TSecr=582503440
Frame 84: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: AmazonTechno_9e:28:73 (3c:5c:c4:9e:28:73), Dst: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:
0a:0a)
Internet Protocol Version 4, Src: 192.168.80.101, Dst: 143.204.150.155
Transmission Control Protocol, Src Port: 44285, Dst Port: 80, Seq: 191, Ack: 498, Len: 0
No.     Time           Source                Destination           Protocol Length Info
     85 27.769680      192.168.80.101        52.216.143.164        TCP      56     55420 → 80
[FIN, ACK] Seq=1 Ack=1 Win=1403 Len=0
Frame 85: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
Ethernet II, Src: AmazonTechno_9e:28:73 (3c:5c:c4:9e:28:73), Dst: 00:ec:ac:cd:0a:0a (00:ec:ac:cd:
0a:0a)
Internet Protocol Version 4, Src: 192.168.80.101, Dst: 52.216.143.164
Transmission Control Protocol, Src Port: 55420, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

Figure 1: Packets 76-85

3 Analysis for Packets 89-91

3.1

Packets 89-91 does not contain any application layer protocol because TCP requires connection establishment before data transmission. In this case, packets 89-91 are used to establish the connection between the client and the server with 3 handshake steps. Then we can find in packet 92 that the application layer protocol is HTTP with is a GET request, which also indicates the connection has been established successfully in the previous 3 packets.

3.2 The closure of this connection

Packet 226 and 227 are correlated with the closure of this connection mentioned above. It can be seen by tracking the sequence number 9 in the filter bar. In packet 226, the server sends a FIN flag to the client to request the closure of the connection. Then in packet 227, the client sends an ACK flag to the server to acknowledge the request.