

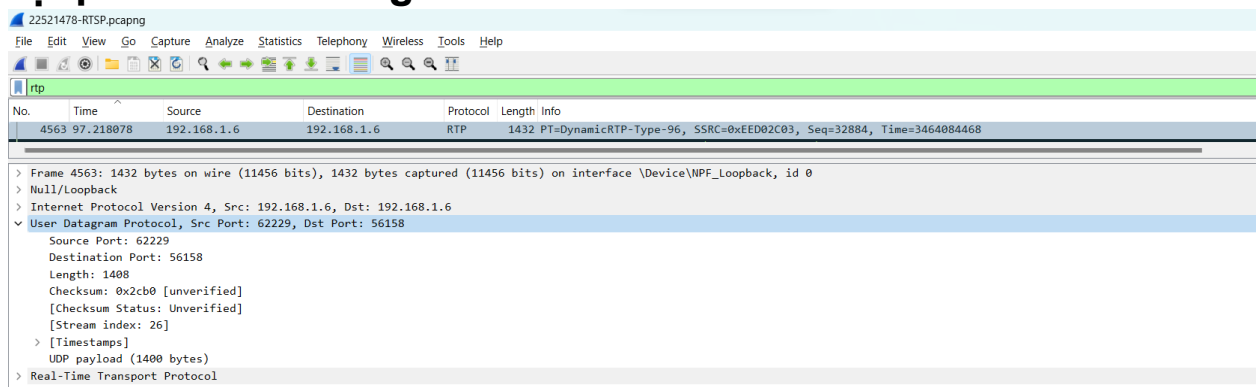
Lab 3 : Phân tích hoạt động giao thức TCP – UDP

Task1 : Phân tích hoạt động giao thức UDP

Ảnh xem Stream VCL :



1. Chọn một gói tin UDP, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó? Gợi ý: Xem tại phần User Datagram Protocol.



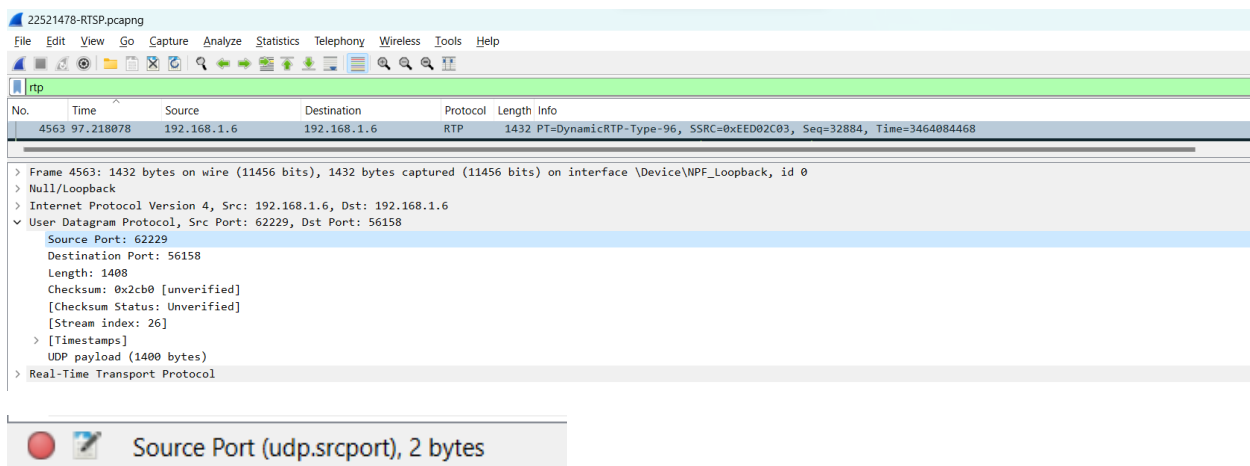
UDP header gồm có 4 trường:

- Source port: Số hiệu cổng nơi đã gửi gói dữ liệu (datagram).
- Destination port: Số hiệu cổng nơi datagram được chuyển tới.

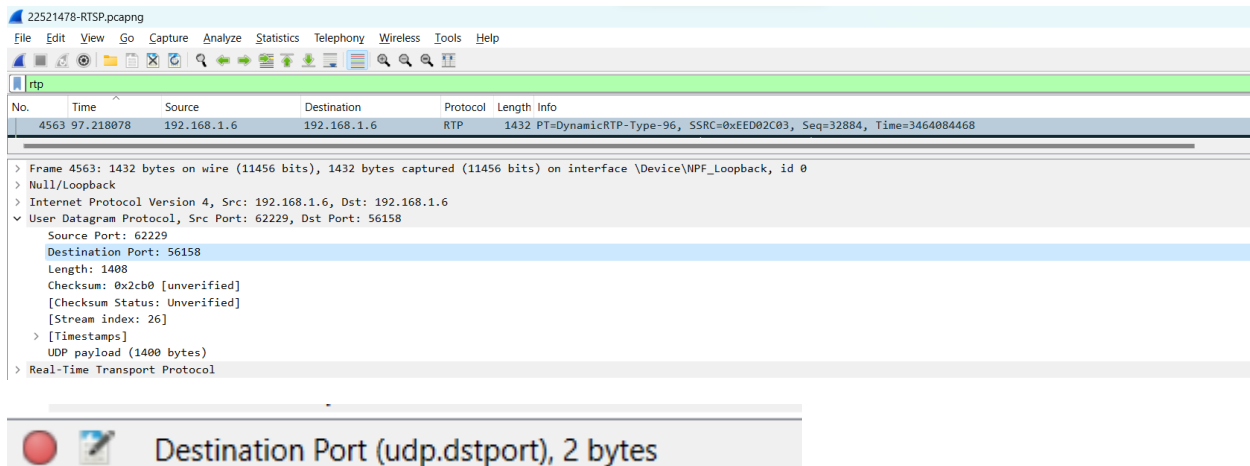
- Length: Độ dài tổng cộng kể cả phần header của gói UDP datagram.-
- Checksum: Trường checksum dùng cho việc kiểm tra lỗi của phần header và dữ liệu, nếu phát hiện lỗi thì UDP datagram sẽ bị loại bỏ mà không có thông báo trả về nơi gửi.

2. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?

Độ dài của mỗi trường trong UDP header là 2 bytes.



Source Port (udp.srcport), 2 bytes



Destination Port (udp.dstport), 2 bytes

22521478-RTSP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

rtsp

No.	Time	Source	Destination	Protocol	Length	Info
4563	97.218078	192.168.1.6	192.168.1.6	RTP	1432	PT=DynamicRTP-Type-96, SSRC=0xEED02C03, Seq=32884, Time=3464084468

> Frame 4563: 1432 bytes on wire (11456 bits), 1432 bytes captured (11456 bits) on interface \Device\NPF_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.6

✓ User Datagram Protocol, Src Port: 62229, Dst Port: 56158

Source Port: 62229

Destination Port: 56158

Length: 1408

Checksum: 0x2cb0 [unverified]

[Checksum Status: Unverified]

[Stream index: 26]

> [Timestamps]

UDP payload (1400 bytes)

> Real-Time Transport Protocol

Length in octets including this header and the data (udp.length), 2 bytes

22521478-RTSP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

rtsp

No.	Time	Source	Destination	Protocol	Length	Info
4563	97.218078	192.168.1.6	192.168.1.6	RTP	1432	PT=DynamicRTP-Type-96, SSRC=0xEED02C03, Seq=32884, Time=3464084468

> Frame 4563: 1432 bytes on wire (11456 bits), 1432 bytes captured (11456 bits) on interface \Device\NPF_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.6

✓ User Datagram Protocol, Src Port: 62229, Dst Port: 56158

Source Port: 62229

Destination Port: 56158

Length: 1408

Checksum: 0x2cb0 [unverified]

[Checksum Status: Unverified]

[Stream index: 26]

> [Timestamps]

UDP payload (1400 bytes)

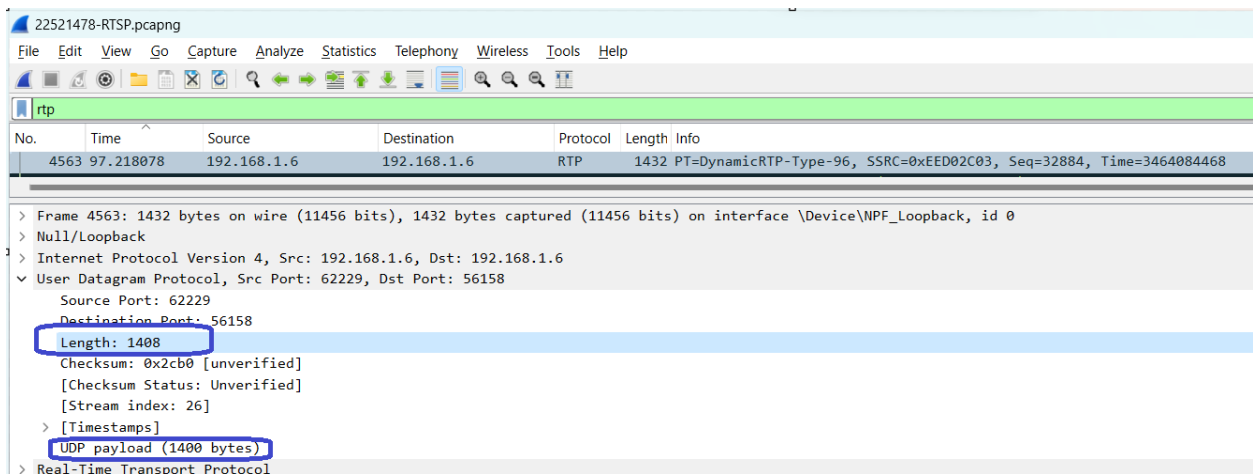
> Real-Time Transport Protocol

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes

3. Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này?

Giá trị của trường Length trong UDP header là độ dài của 8 bytes UDP header cộng với 1400 bytes của data (UDP payload) tương đương với độ dài 1408 bytes.

$$\text{Length} = \text{UDP payload} + 8 \text{ bytes} = 1400 + 8 = 1408$$



4. Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa?

Số bytes tối đa mà UDP payload có thể chứa là $2^{16} - 1$ trừ đi 8 bytes của header, tức là $65535 - 8 = 65527$ bytes

5. Giá trị lớn nhất có thể có của port nguồn (Source port)?

Giá trị lớn nhất có thể có của port nguồn (Source port) là $2^{16} - 1 = 65535$

6. * Tìm và kiểm tra một cặp gói tin sử dụng giao thức UDP gồm: gói tin do máy mình gửi và gói tin phản hồi của gói tin đó. Miêu tả mối quan hệ về port number của 2 gói tin này.

-Hai gói tin số 411 và 545:

411	48.607353	172.20.10.3	172.20.10.7	RTCP	106 Sender Report	Source description
545	50.204955	172.20.10.7	172.20.10.3	RTCP	102 Receiver Report	Source description

- Gói tin 441 :

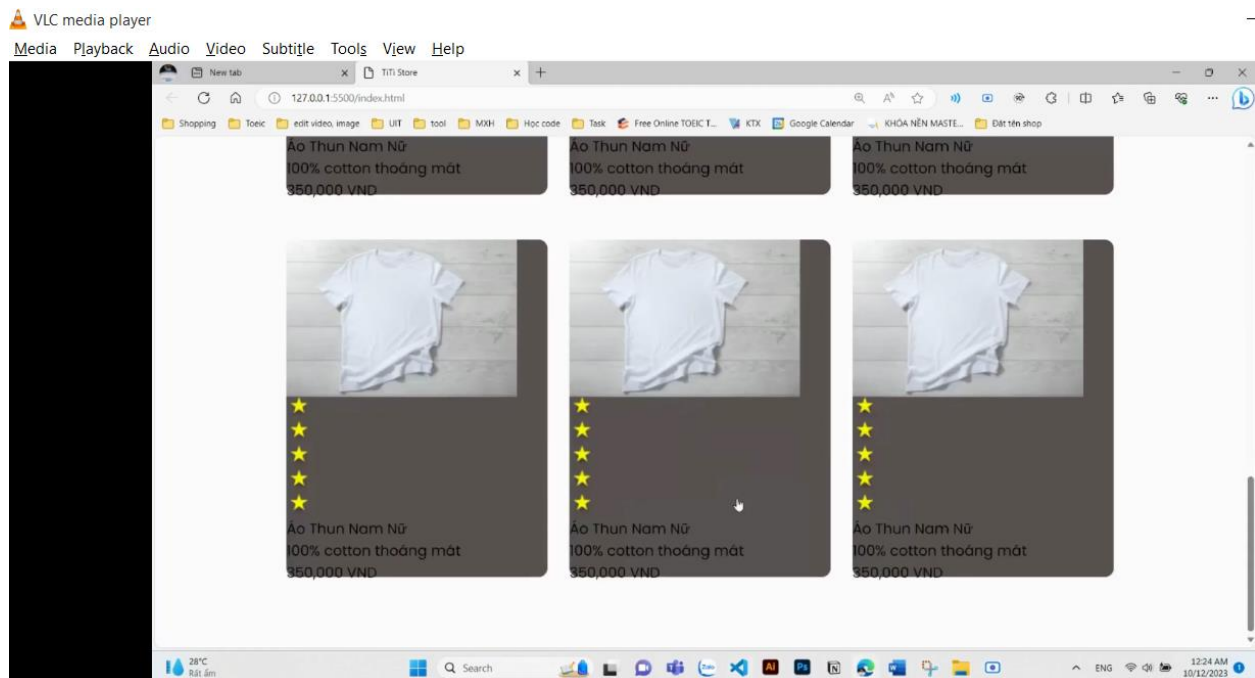
```
> Frame 411: 106 bytes on wire (848 bits), 106 bytes captured
> Ethernet II, Src: CloudNet_59:18:a5 (5c:61:99:59:18:a5),
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 172.20.10.7
> User Datagram Protocol, Src Port: 56307, Dst Port: 54365
  Source Port: 56307
  Destination Port: 54365
```

- Gói 545 :

```
> Frame 545: 102 bytes on wire (816 bits), 102 bytes captured  
> Ethernet II, Src: IntelCor_73:c4:6d (f4:26:79:73:c4:6d),  
> Internet Protocol Version 4, Src: 172.20.10.7, Dst: 172.16.17.1  
✓ User Datagram Protocol, Src Port: 54365, Dst Port: 56307  
    Source Port: 54365  
    Destination Port: 56307
```

+ Mối quan hệ: Port nguồn của gói UDP bên gửi giống port đích của gói UDP phản hồi và ngược lại

Task 2: Phân tích hoạt động giao thức TCP



7. Tìm địa chỉ IP và TCP port của máy Client?

22521478-TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
38	55.523151	192.168.1.6	192.168.1.6	HTTP	163	OPTIONS rtsp://192.168.1.6:8
40	55.556600	192.168.1.6	192.168.1.6	HTTP	169	Continuation
42	55.559492	192.168.1.6	192.168.1.6	HTTP	189	Continuation
44	55.587435	192.168.1.6	192.168.1.6	HTTP	116	Continuation
46	55.587702	192.168.1.6	192.168.1.6	HTTP	356	Continuation
70	55.672079	192.168.1.6	192.168.1.6	HTTP	379	OPTIONS rtsp://192.168.1.6:8
72	55.696507	192.168.1.6	192.168.1.6	HTTP	169	Continuation
124	182.166797	192.168.1.6	192.168.1.6	HTTP	178	GET / HTTP/1.1
2033	262.023106	192.168.1.6	192.168.1.6	HTTP	178	GET / HTTP/1.1
3248	311.117058	192.168.1.6	192.168.1.6	HTTP	178	GET / HTTP/1.1
4619	351.577693	192.168.1.6	192.168.1.6	HTTP	178	GET / HTTP/1.1

> Frame 124: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits) on interface \Device\NPF{...}

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.6

> Transmission Control Protocol, Src Port: 49926, Dst Port: 8080, Seq: 1, Ack: 1, Len: 13

Source Port: 49926

Destination Port: 8080

IP của máy Client: 192.168.1.6

TCP port của máy Client: 49926

8. Tìm địa chỉ IP của Server? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?

22521478-TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
120	181.737341	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK]
121	182.160019	192.168.1.6	192.168.1.6	TCP	56	49926 → 8080 [SYN] Seq: 1
122	182.160077	192.168.1.6	192.168.1.6	TCP	56	8080 → 49926 [SYN, ACK] Seq: 1, Win: 0

> Frame 122: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF{...}

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.6

> Transmission Control Protocol, Src Port: 8080, Dst Port: 49926, Seq: 0, Ack: 1, Len: 0

Source Port: 8080

Destination Port: 49926

- Địa chỉ IP của Server : 192.168.1.6

- TCP port : 8080

9. TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?

The image shows a Wireshark packet capture window titled "22521478-TCP.pcapng". The packet list on the left shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
120	181.737341	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK]
121	182.160019	192.168.1.6	192.168.1.6	TCP	56	49926 → 8080 [SYN] Seq: 0
122	182.160077	192.168.1.6	192.168.1.6	TCP	56	8080 → 49926 [SYN, ACK]

The packet details pane on the right shows the structure of packet 121:

- > Frame 121: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF...
- > Null/Loopback
- > Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.6
- ✓ Transmission Control Protocol, Src Port: 49926, Dst Port: 8080, Seq: 0, Len: 0
 - Source Port: 49926
 - Destination Port: 8080
 - [Stream index: 5]
 - > [Conversation completeness: Complete, WITH_DATA (63)]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 2405807622
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 0
 - Acknowledgment number (raw): 0
 - 1000 = Header Length: 32 bytes (8)
 - ✓ Flags: 0x002 (SYN)
 - 000. = Reserved: Not set
 - ...0 = Accurate ECN: Not set
 - 0... = Congestion Window Reduced: Not set
 -0.. = ECN-Echo: Not set
 -0. = Urgent: Not set
 -0 = Acknowledgment: Not set
 - 0.. = Push: Not set
 -0.. = Reset: Not set
 - >1. = Syn: Set
 -0 = Fin: Not set
 - [TCP Flags:S.]
 - Window: 65535
 - [Calculated window size: 65535]
 - Checksum: 0xc98c [unverified]
 - [Checksum Status: Unverified]

TCP SYN segment sử dụng sequence number là 0 vì nó được sử dụng để khởi tạo kết nối TCP giữa máy client và server.

Trong trường Flags, SYN flag được đặt thành 1 cho biết rằng segment này là một TCP SYN segment.

10. Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment? Tìm giá trị của Acknowledgement trong SYN/ACK segment? Làm sao server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYN/ACK segment?

22521478-TCP.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
120	181.737341	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK]
121	182.160019	192.168.1.6	192.168.1.6	TCP	56	49926 → 8080 [SYN] Seq=0
122	182.160077	192.168.1.6	192.168.1.6	TCP	56	8080 → 49926 [SYN, ACK] Seq=0, Win=65535, Len=0

> Frame 122: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF{...}

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.1.6, Dst: 192.168.1.6

▼ Transmission Control Protocol, Src Port: 8080, Dst Port: 49926, Seq: 0, Ack: 1, Len: 0

Source Port: 8080

Destination Port: 49926

[Stream index: 5]

> [Conversation completeness: Complete, WITH_DATA (63)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 1543896401

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 2405807623

1000 = Header Length: 32 bytes (8)

▼ Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Accurate ECN: Not set

.... 0... = Congestion Window Reduced: Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

.... 0... = Push: Not set

.... 0.. = Reset: Not set

>1. = Syn: Set

....0 = Fin: Not set

[TCP Flags:A..S.]

Window: 65535

[Calculated window size: 65535]

Checksum: 0x7024 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

0000 02 00
0010 c0 a8
0020 8f 65
0030 01 03

- Sequence number của gói tin SYN/ACK segment do server gửi đến máy client để trả lời cho SYN segment là 0.
- Giá trị của trường Acknowledgement trong SYN/ACK segment là 1.
- Một segment sẽ được xác định là SYN/ACK segment nếu cả giá trị SYN flag và Acknowledgement flag trong segment được đặt thành 1.

11. Chỉ ra 6 segment đầu tiên mà server gửi cho Client (dựa vào Số thứ tự gói –No)

- Tìm sequence number của 6 segments đầu tiên đó?
 - Xác định thời gian mà mỗi segment được gửi, thời gian ACK cho mỗi segment được nhận?
 - Đưa ra sự khác nhau giữa thời gian mà mỗi segment được gửi và thời gian ACK cho mỗi segment được nhận bằng cách tính RTT (Round Trip Time) cho 6 segments này?
- 6 segments đầu tiên mà server gửi cho Client: 5, 7, 9, 10, 12, 13
- Sequence number của 6 segments đầu tiên lần lượt là: 1, 104, 496, 1956, 3416, 4876

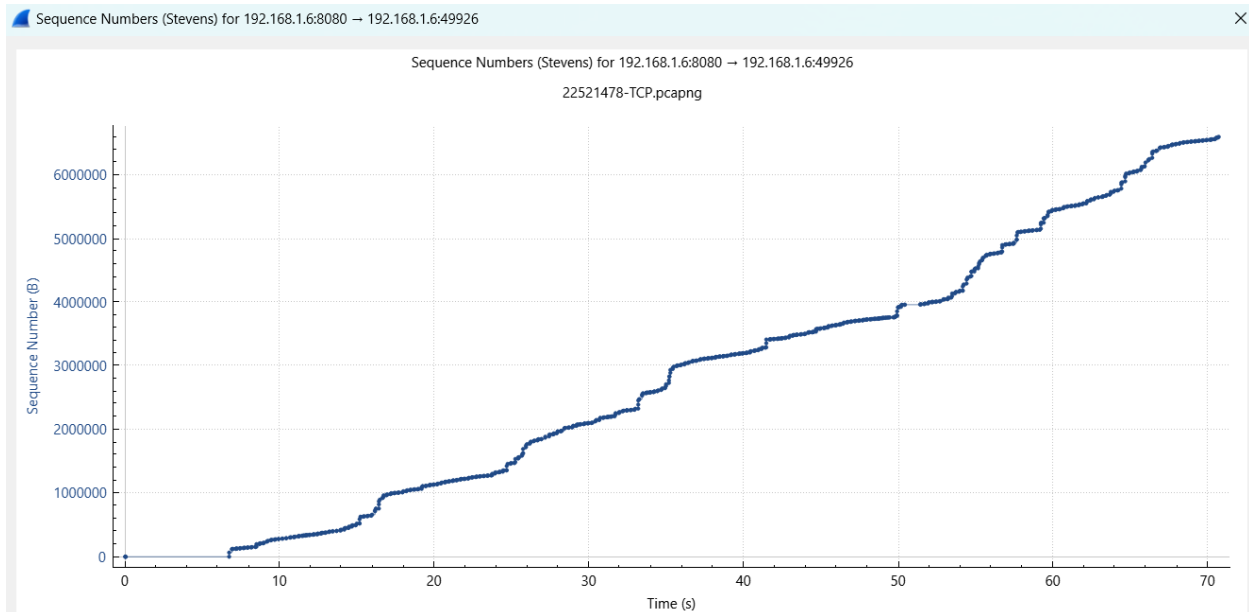
No.	Time	Source	Destination	Protocol	Length	Info
2	0.000385	192.168.188.128	192.168.188.1	TCP	66	8080 → 28299 [SYN, ACK] Seq=0 Ack=1 Win=655...
5	0.024509	192.168.188.128	192.168.188.1	TCP	157	8080 → 28299 [PSH, ACK] Seq=1 Ack=136 Win=2...
7	0.064611	192.168.188.128	192.168.188.1	TCP	446	8080 → 28299 [PSH, ACK] Seq=104 Ack=136 Win...
9	2.125153	192.168.188.128	192.168.188.1	TCP	1514	8080 → 28299 [ACK] Seq=496 Ack=136 Win=2102...
10	2.125289	192.168.188.128	192.168.188.1	TCP	1514	8080 → 28299 [ACK] Seq=1956 Ack=136 Win=210...
12	2.125336	192.168.188.128	192.168.188.1	TCP	1514	8080 → 28299 [ACK] Seq=3416 Ack=136 Win=210...
13	2.125363	192.168.188.128	192.168.188.1	TCP	1514	8080 → 28299 [ACK] Seq=4876 Ack=136 Win=210...
15	2.125386	192.168.188.128	192.168.188.1	TCP	1514	8080 → 28299 [ACK] Seq=6336 Ack=136 Win=210...
16	2.125408	192.168.188.128	192.168.188.1	TCP	1514	8080 → 28299 [ACK] Seq=7796 Ack=136 Win=210...

No.	Time	Source	Destination	Protocol	Length	Info
6	0.064392	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=104 Win=1050...
8	0.106979	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=496 Win=1050...
11	2.125320	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=3416 Win=105...
14	2.125377	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=6336 Win=105...
17	2.125422	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=9256 Win=105...
19	2.169665	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=9338 Win=105...
22	2.170100	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=12258 Win=10...
25	2.170138	192.168.188.1	192.168.188.128	TCP	54	28299 → 8080 [ACK] Seq=136 Ack=15178 Win=10...

STT	Thời Gian Gửi	Thời Gian Nhận ACK	RTT (Round Trip Time)
1	0.024509	0.064392	0.039883

2	0.064611	0.106979	0.042368
3	2.125153	2.125320	0.000167
4	2.125289	2.125377	0.000088
5	2.125336	2.125422	0.000086
6	2.125363	2.169665	0.044302

12. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó?



Không có segment nào được gửi lại. Điều này có thể được giải thích bởi các gói có cùng sequence number tại các thời điểm khác nhau không được tìm thấy.