

## BÁO CÁO THỰC HÀNH

**Môn học:** Nhập môn mạng máy tính

**Buổi báo cáo:** Lab 3

**Tên chủ đề:** Làm quen với Wireshark

*GVHD: Phan Trung Phát*

*Ngày thực hiện: 30/10/2022*

*Ngày nộp báo cáo: 30/10/2022*

### 1. THÔNG TIN CHUNG:

Lớp: IT005.N11.KHTN.1

ST T	Họ và tên	MSSV	Email
1	Lương Toàn Bách	21521845	21521845@gm.uit.edu.vn

### 2. ĐÁNH GIÁ KHÁC:

Nội dung	Kết quả
Tổng thời gian thực hiện bài thực hành trung bình	1.5 tiếng
Link Video thực hiện (nếu có)	Không có
Ý kiến (nếu có) + Khó khăn + Đề xuất ...	Không có
Điểm tự đánh giá	9.0

**Phần bên dưới của báo cáo này là báo cáo chi tiết của nhóm thực hiện.**

### BÁO CÁO CHI TIẾT

---

*Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này*

## I. Phân tích gói tin UDP

The screenshot displays two windows side-by-side. On the left is the Wireshark network protocol analyzer, showing a packet capture from a Wi-Fi interface. The packet list on the left shows several packets, with packet 32 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. On the right is the VLC media player window, which is playing a video. The video frame shows a close-up of a piece of paper with handwritten text in Vietnamese. The text reads: "Yêu em như là lần cuối / Cơn buồn nào mà chớ gần gũi". The VLC media player interface includes standard playback controls and a progress bar.

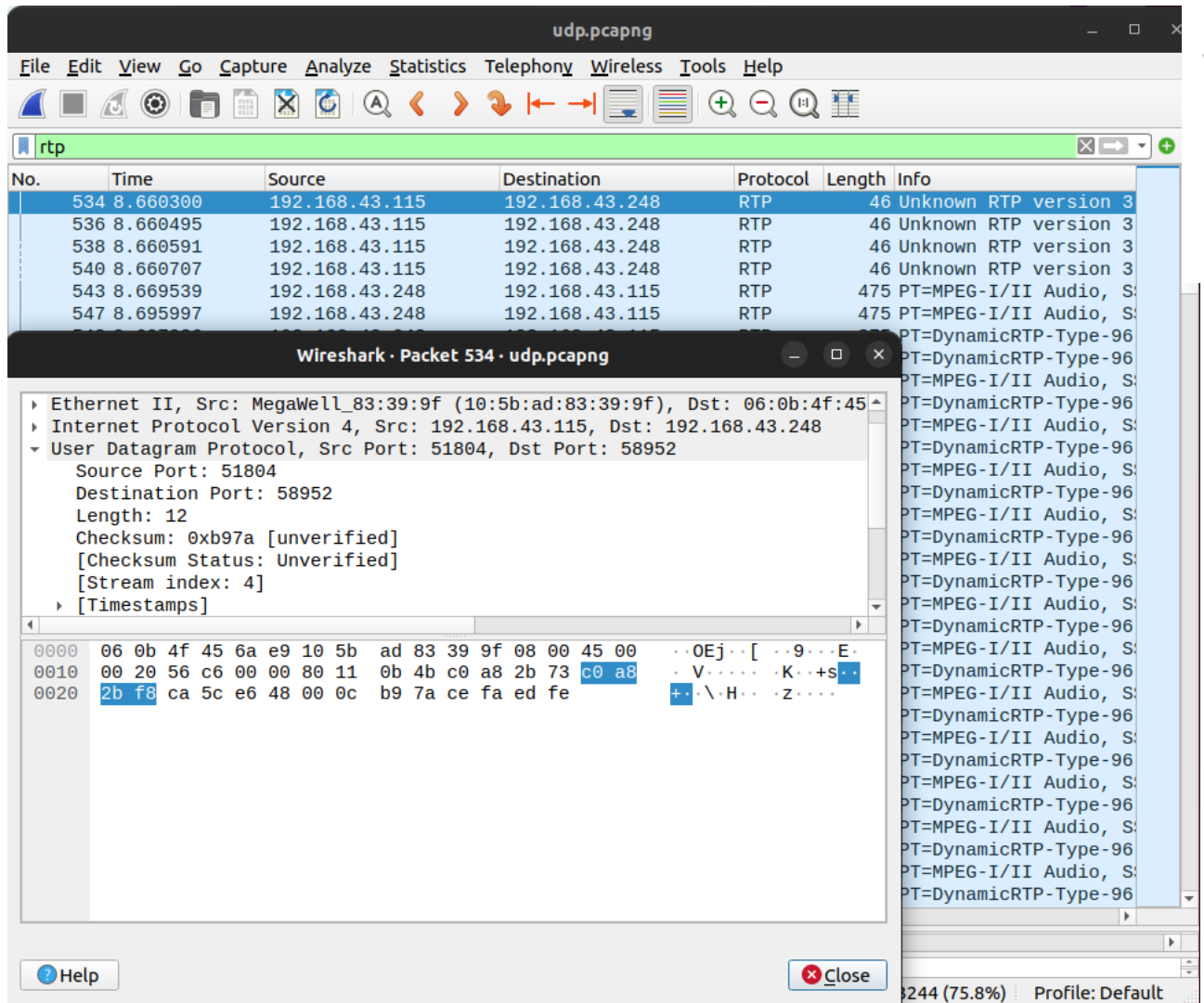
No.	Time	Source
27	2.155575	192.168.43.115
30	2.402433	192.168.43.248
31	2.402497	192.168.43.115
32	2.413471	192.168.43.115
42	2.583583	192.168.43.248
51	2.634721	192.168.43.115
54	2.646930	192.168.43.248
55	2.698228	192.168.43.115
63	4.665964	192.168.43.248
64	4.665964	192.168.43.248

Frame 27: 66 bytes on wire (528 bits)  
Ethernet II, Src: Megalini, 83:39:9f (3)  
Internet Protocol Version 4, Src: 192.168.43.115, Dst: 192.168.43.248  
Transmission Control Protocol, Src Port: 54321, Dst Port: 54321

0000 06 0b 4f 45 6a e9 10 5b ad 83 39  
0010 00 34 56 f2 40 00 80 06 cb 15 c0  
0020 2b f8 d1 86 1f 90 a5 57 9e c0 00  
0030 fa f0 65 34 00 00 02 04 05 b4 01  
0040 04 02

Yêu em như là lần cuối  
Cơn buồn nào mà chớ gần gũi

**Câu 1:** Chọn một gói tin UDP, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó?



- + Source port: Cổng của thiết bị gửi đi
- + Destination port: Cổng của thiết bị nhận được
- + Length: Kích thước của gói tin
- + Checksum: Kiểm tra lỗi của phần header và dữ liệu

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

Source Port (udp.srcport), 2 bytes

Destination Port (udp.dstport), 2 bytes

Length (udp.length), 2 bytes

Details at: [https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChAdvChecksums.html](https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html) (udp.checksum), 2 bytes

Mọi trường trong UDP head đều có độ dài là 2 bytes

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

The image shows a Wireshark packet capture window titled 'udp.pcapng'. The packet list on the left shows several SSDP packets. Packet 1168 is selected, and its details are shown in the right pane. The details pane shows the 'User Datagram Protocol' section with the following fields:

- Source Port: 62823
- Destination Port: 1900
- Length: 109
- Checksum: 0x9f0f [unverified]
- [Checksum Status: Unverified]
- [Stream index: 9]
- [Timestamps]
- UDP payload (101 bytes)
- Simple Service Discovery Protocol

The packet bytes pane at the bottom shows the raw data of the packet, with the first 8 bytes (0000 to 0007) highlighted in blue, corresponding to the UDP header fields.

- Giá trị của trường Length trong UDP header là độ dài của toàn bộ datagram (header + data)
- Chứng minh: Trong trường hợp này trường Length = 109 (header = 8 + data = 101)

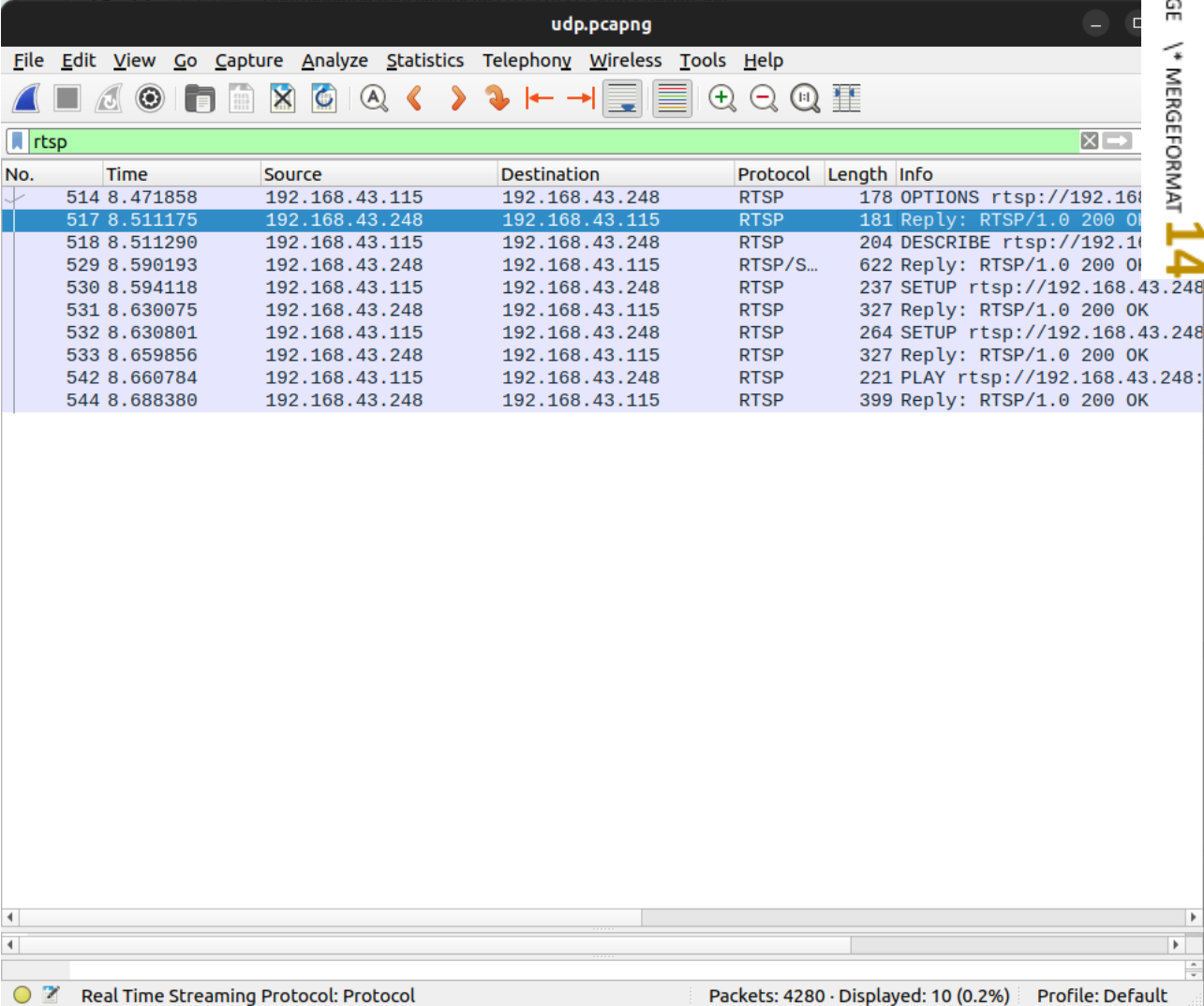
**Câu 4: Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa?**

- Với trường kích thước 2 bytes, kích thước lớn nhất mà payload của UDP có thể chứa là  $2^{16} - 1 - 8 = 65527$  bytes. (trừ thêm 8 bytes của header)

**Câu 5: Giá trị lớn nhất có thể có của port nguồn (Source port)?**

- Giá trị lớn nhất có thể có của port nguồn là  $2^{16} - 1$

**Câu 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.**



The image shows a Wireshark packet capture window titled 'udp.pcapng'. The filter bar at the top is set to 'rtsp'. The packet list pane displays a series of RTSP packets. Packet 514 is selected, showing its details in the packet details pane. The status bar at the bottom indicates 'Real Time Streaming Protocol: Protocol', 'Packets: 4280 · Displayed: 10 (0.2%)', and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
514	8.471858	192.168.43.115	192.168.43.248	RTSP	178	OPTIONS rtsp://192.168.43.248:554
517	8.511175	192.168.43.248	192.168.43.115	RTSP	181	Reply: RTSP/1.0 200 OK
518	8.511290	192.168.43.115	192.168.43.248	RTSP	204	DESCRIBE rtsp://192.168.43.248:554
529	8.590193	192.168.43.248	192.168.43.115	RTSP/S...	622	Reply: RTSP/1.0 200 OK
530	8.594118	192.168.43.115	192.168.43.248	RTSP	237	SETUP rtsp://192.168.43.248:554
531	8.630075	192.168.43.248	192.168.43.115	RTSP	327	Reply: RTSP/1.0 200 OK
532	8.630801	192.168.43.115	192.168.43.248	RTSP	264	SETUP rtsp://192.168.43.248:554
533	8.659856	192.168.43.248	192.168.43.115	RTSP	327	Reply: RTSP/1.0 200 OK
542	8.660784	192.168.43.115	192.168.43.248	RTSP	221	PLAY rtsp://192.168.43.248:554
544	8.688380	192.168.43.248	192.168.43.115	RTSP	399	Reply: RTSP/1.0 200 OK

- Chọn gói tin số 514 và 517

Gói tin request

The image shows a Wireshark packet capture of an RTSP session. The main window displays a list of packets, and a detailed view of packet 514 is shown below it.

No.	Time	Source	Destination	Protocol	Length	Info
514	8.471858	192.168.43.115	192.168.43.248	RTSP	178	OPTIONS rtsp://192.168.43.248:8554/ RTSP/1.0\r\n
517	8.511175	192.168.43.248	192.168.43.115	RTSP	181	Reply: RTSP/1.0 200 OK
518	8.511290	192.168.43.115	192.168.43.248	RTSP	204	DESCRIBE rtsp://192.168.43.248:8554/ RTSP/1.0\r\n
529	8.590193	192.168.43.248	192.168.43.115	RTSP/S...	622	Reply: RTSP/1.0 200 OK
530	8.594118	192.168.43.115	192.168.43.248	RTSP	237	SETUP rtsp://192.168.43.248:8554/ RTSP/1.0\r\n
531	8.630075	192.168.43.248	192.168.43.115	RTSP	327	Reply: RTSP/1.0 200 OK

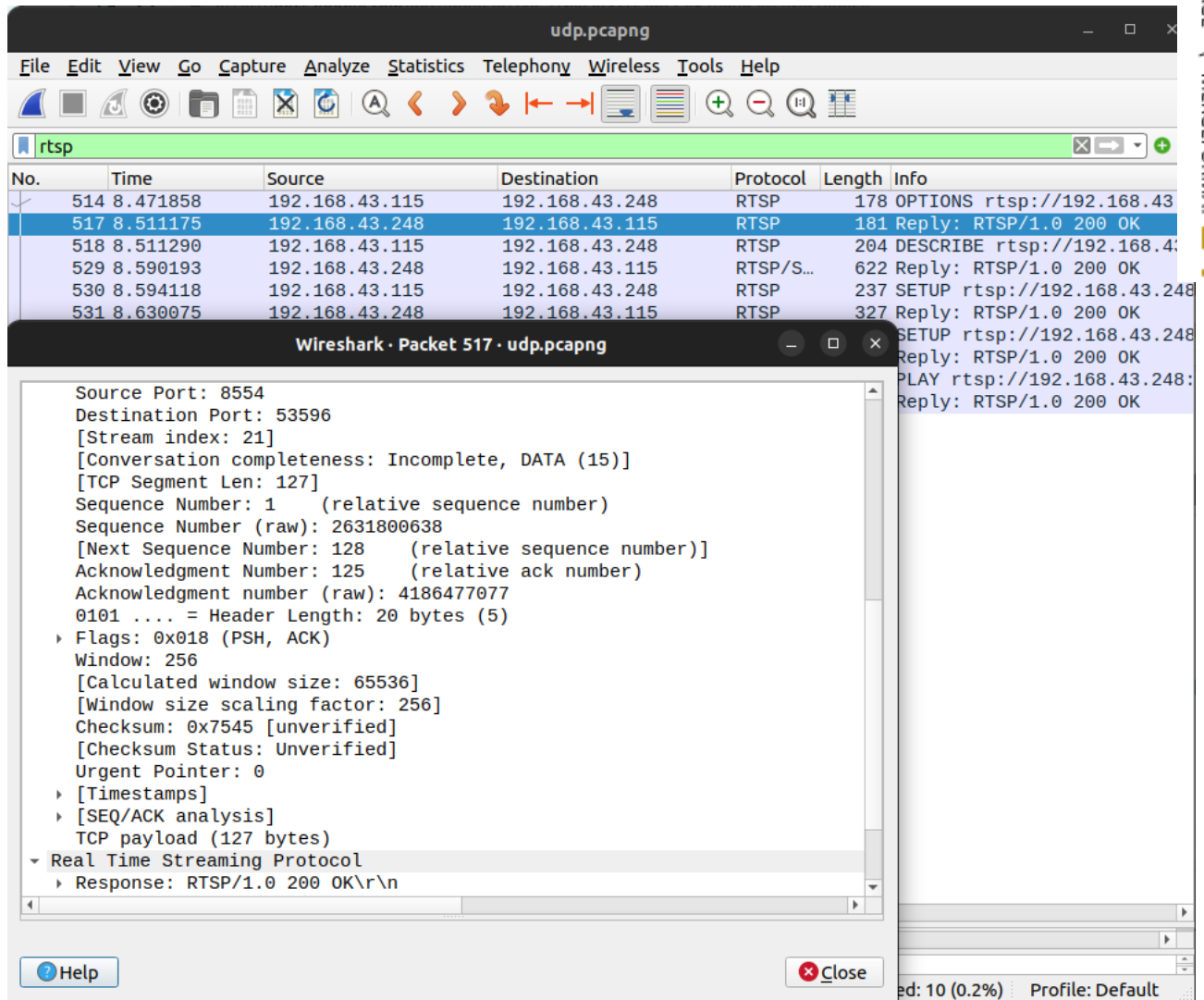
**Wireshark · Packet 514 · udp.pcapng**

Source Port: 53596  
 Destination Port: 8554  
 [Stream index: 21]  
 [Conversation completeness: Incomplete, DATA (15)]  
 [TCP Segment Len: 124]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 4186476953  
 [Next Sequence Number: 125 (relative sequence number)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 2631800638  
 0101 .... = Header Length: 20 bytes (5)  
 ▶ Flags: 0x018 (PSH, ACK)  
 Window: 256  
 [Calculated window size: 65536]  
 [Window size scaling factor: 256]  
 Checksum: 0x2c5b [unverified]  
 [Checksum Status: Unverified]  
 Urgent Pointer: 0  
 ▶ [Timestamps]  
 ▶ [SEQ/ACK analysis]  
 TCP payload (124 bytes)  
 ▶ Real Time Streaming Protocol  
 ▶ Request: OPTIONS rtsp://192.168.43.248:8554/ RTSP/1.0\r\n

Help Close

ed: 10 (0.2%) Profile: Default

Gói tin response



- Port number của 2 gói tin này ngược nhau.
  - Gói tin request có source port = 53596, destination port = 8554.
  - Gói tin response có source port = 8554, destination port = 53596.

## II. Phân tích hoạt động giao thức TCP

### Câu 7: Tìm địa chỉ IP và TCP port của máy Client?



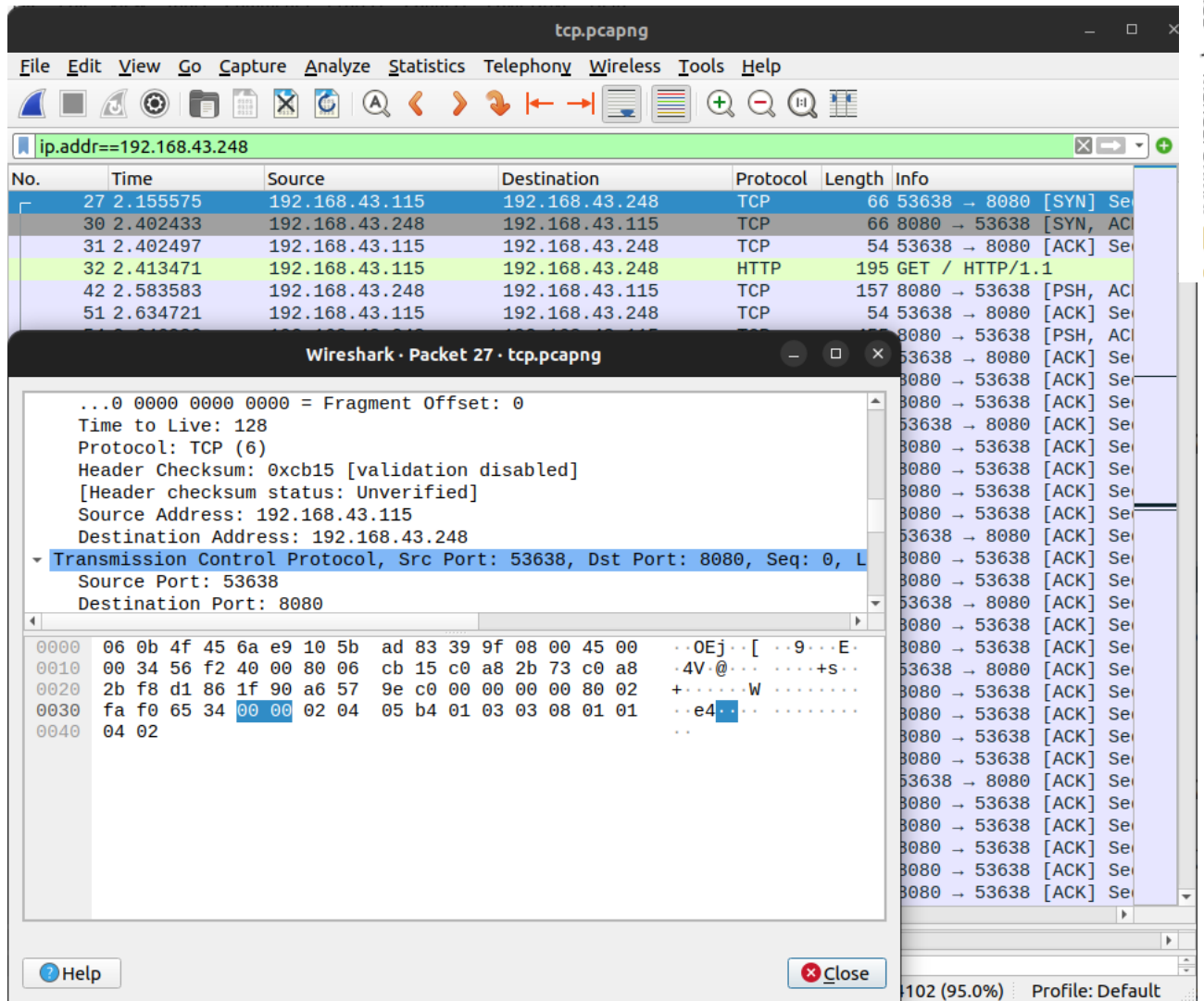
The image shows a Wireshark packet capture analysis of a file named `tcp.pcapng`. The main packet list displays several packets, with packet 27 selected. The packet details pane shows the following information for packet 27:

- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 128
- Protocol: TCP (6)
- Header Checksum: 0xcb15 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.43.115
- Destination Address: 192.168.43.248
- Transmission Control Protocol, Src Port: 53638, Dst Port: 8080, Seq: 0, Len: 0
- Source Port: 53638
- Destination Port: 8080

The packet bytes pane shows the raw data of the packet, including the IP header and the TCP header.

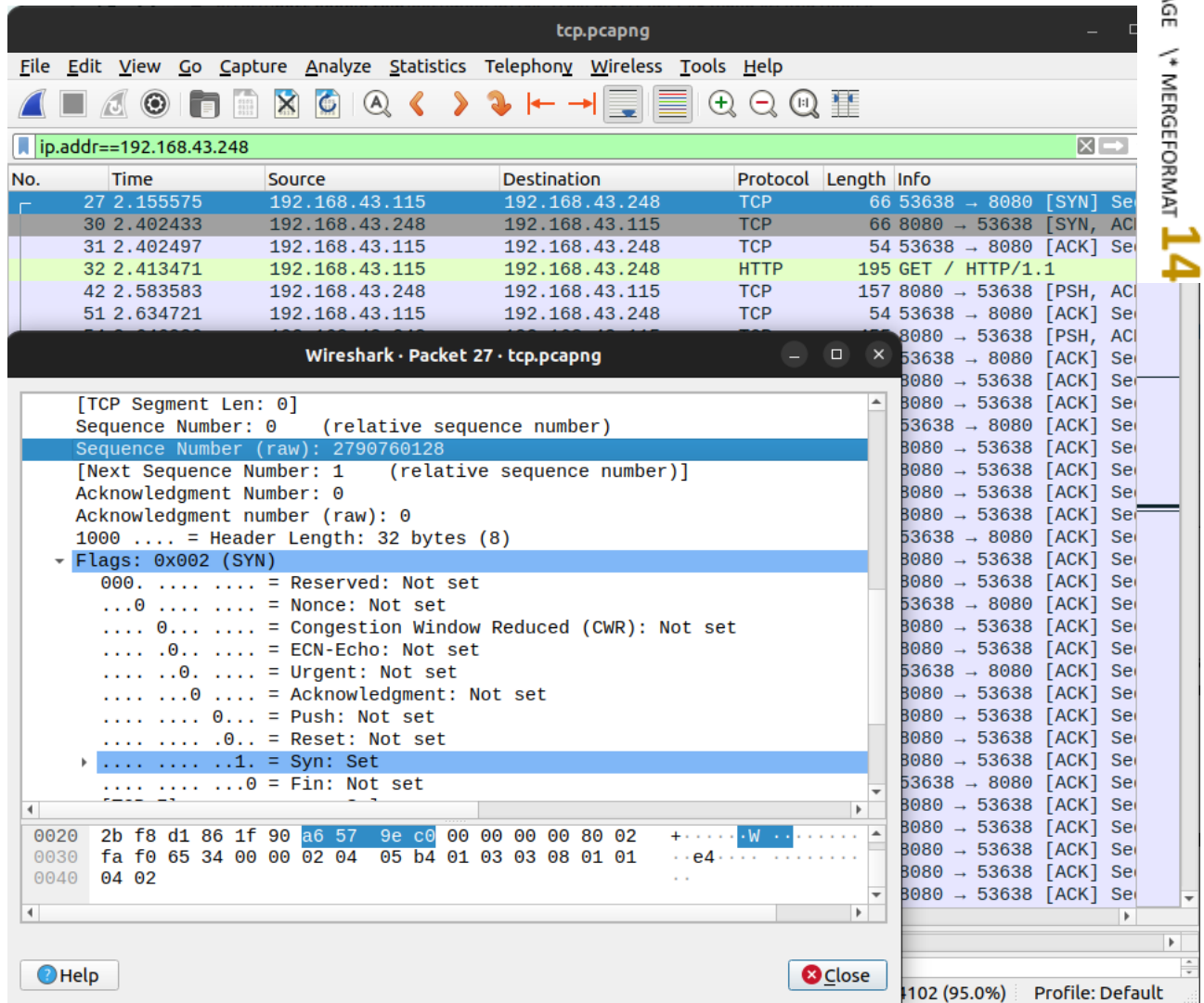
- Địa chỉ IP của máy Client: 192.168.43.115
- TCP port: 53638

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



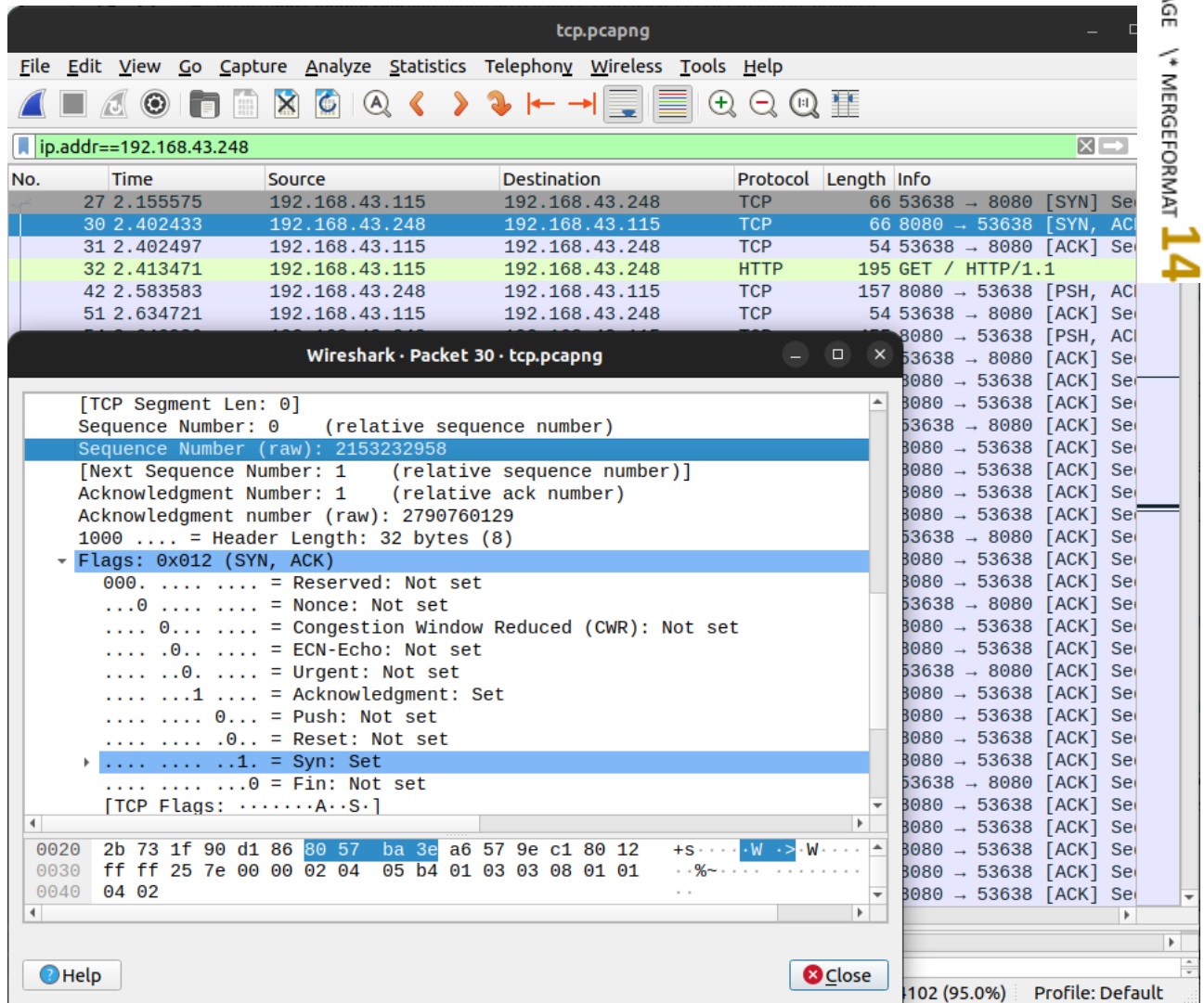
- Địa chỉ IP của Server: 192.168.43.248
- TCP port: 8080

**Câu 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?



- TCP SYN segment (gói tin TCP có cờ SYN) sử dụng SEQ = 2790760128 để khởi tạo kết nối TCP giữa client và server
- Thành phần trong segment cho ta biết segment đó là TCP SYN segment là: SYN = 1

**Câu 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?



- SEQ của gói tin SYN/ACK là: 2153232958
- Giá trị của acknowledgement trong SYN/ACK là: 2790760129
- Thành phần trong segment cho ta biết segment đó là SYN/ACK segment là: Bit của trường ACK và SYN đều bằng 1

**Câu 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 ?

tcp.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.43.248

No.	Time	Source	Destination	Protocol	Length	Info
30	2.402433	192.168.43.248	192.168.43.115	TCP	66	8080 → 53638 [SYN, AC
42	2.583583	192.168.43.248	192.168.43.115	TCP	157	8080 → 53638 [PSH, AC
54	2.646930	192.168.43.248	192.168.43.115	TCP	455	8080 → 53638 [PSH, AC
63	4.665964	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
64	4.665964	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
66	4.675229	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
67	4.678162	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
68	4.678162	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
69	4.678162	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
71	4.682524	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
72	4.682524	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
74	4.689440	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
75	4.691495	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
77	4.696139	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
78	4.707892	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
79	4.707892	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
80	4.707892	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
82	4.708007	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
83	4.708007	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
84	4.708007	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
85	4.708007	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
86	4.708007	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
87	4.708007	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
89	4.714821	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
90	4.714821	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
91	4.714821	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
92	4.714821	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
94	4.714958	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
95	4.722316	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
96	4.722316	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
97	4.722316	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se
98	4.722316	192.168.43.248	192.168.43.115	TCP	1514	8080 → 53638 [ACK] Se

tcp.pcapng Packets: 4317 · Displayed: 2901 (67.2%) Profile: Default



tcp.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.43.115 && ip.dst==192.168.43.248

No.	Time	Source	Destination	Protocol	Length	Info
27	2.155575	192.168.43.115	192.168.43.248	TCP	66	53638 → 8080 [SYN] Seq
31	2.402497	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
32	2.413471	192.168.43.115	192.168.43.248	HTTP	195	GET / HTTP/1.1
51	2.634721	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
55	2.698228	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
65	4.666019	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
70	4.678225	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
73	4.682578	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
76	4.691524	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
81	4.707945	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
88	4.708038	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
93	4.714894	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
101	4.722386	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
113	4.730480	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
123	4.740285	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
126	4.741938	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
128	4.743209	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
135	4.749374	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
141	4.760132	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
143	4.761283	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
148	4.764684	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
152	4.787468	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
156	4.895546	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
158	4.995072	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
161	4.997609	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
166	5.114928	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
169	5.230314	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
172	5.231125	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
176	5.394747	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
179	5.457720	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
181	5.510023	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq
189	5.983720	192.168.43.115	192.168.43.248	TCP	54	53638 → 8080 [ACK] Seq

Destination Address: IPv4 address      Packets: 4317 · Displayed: 1201 (27.8%)      Profile: Default

- 6 segments đầu tiên mà server gửi cho Client là: 42, 54, 63, 64, 66, 67
- SEQ của 6 segments lần lượt là: 1, 104, 505, 1965, 3425, 4885

STT	Thời gian gửi	Thời gian nhận ACK	RTT
1	2.583583	2.634721	0.051138
2	2.646930	2.698228	0.051298
3	4.665964	4.666019	0.000055
4	4.665964	4.678225	0.012261
5	4.675229	4.682578	0.007349
6	4.678162	4.691524	0.013362

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

- Có segment gửi lại
- Dựa vào sequence number

