

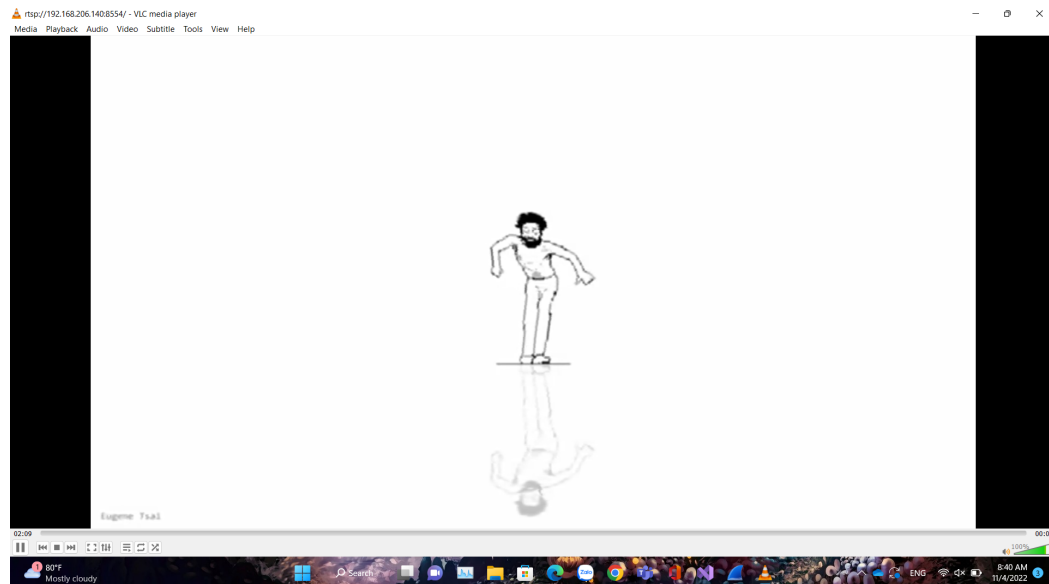
**MSSV:** 21521924 - 21522820

**Họ tên:** Ngô Phúc Danh - Nguyễn Mỹ Hạnh

**Lớp:** IT005.N16

### Lab 3

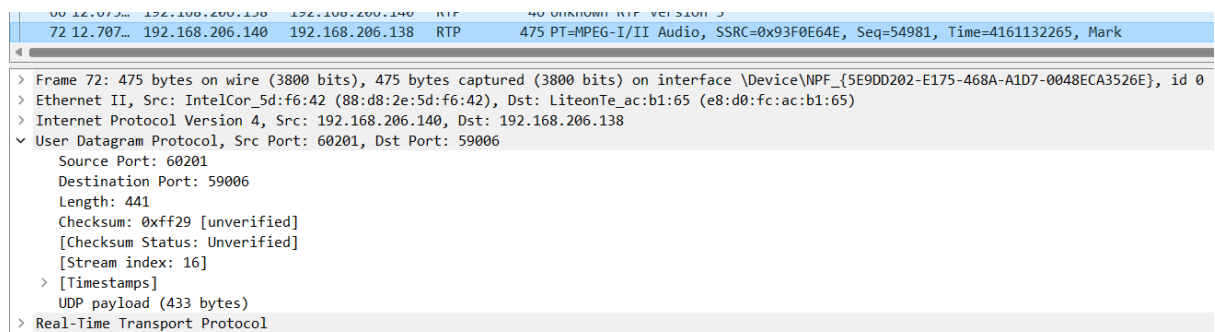
Hình stream video RTSP.



**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?**

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.



**Hình 1.** Các trường trong UDP header

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

Độ dài mỗi trường trong UDP header là 2 bytes.

▼ User Datagram Protocol, Src Port: 60201, Dst Port: 59006

Source Port: 60201

Destination Port: 59006

Length: 441

Checksum: 0xff29 [unverified]

[Checksum Status: Unverified]

[Stream index: 16]

> [Timestamps]

UDP payload (433 bytes)

> Real-Time Transport Protocol

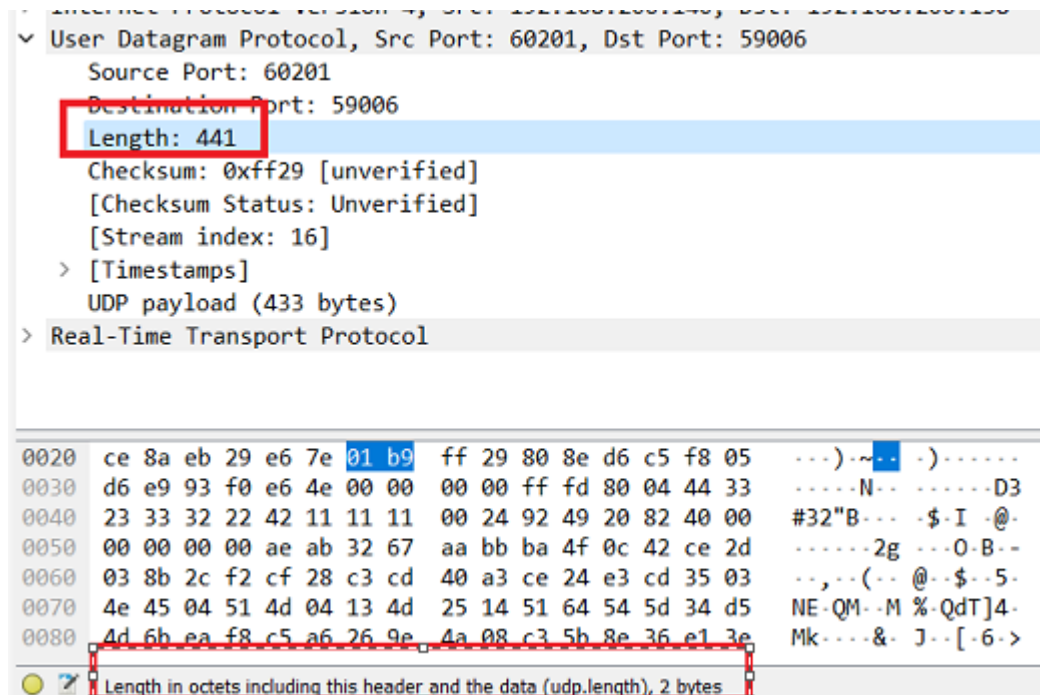
0020	ce 8a eb 29 e6 7e 01 b9 ff 29 80 8e d6 c5 f8 05	... ) ~ ... ) ...
0030	d6 e9 93 f0 e6 4e 00 00 00 00 ff fd 80 04 44 33	... N ... D3
0040	23 33 32 22 42 11 11 11 00 24 92 49 20 82 40 00	#32"B... \$.I .@.
0050	00 00 00 00 ae ab 32 67 aa bb ba 4f 0c 42 ce 2d	... 2g ... O .B .-
0060	03 8b 2c f2 cf 28 c3 cd 40 a3 ce 24 e3 cd 35 03	.., .. ( .. @ .. \$ .. 5.
0070	4e 45 04 51 4d 04 13 4d 25 14 51 64 54 5d 34 d5	NE .QM .M % .QdT]4.
0080	4d 6b ea f8 c5 a6 26 9e 4a 08 c3 5b 8e 36 e1 3e	Mk ... & . J ... [ .6 .>
0090	17 35 76 6b 5a da d9 ce 6b 60 d3 1d 90 53 62 a3	.5vkZ ... k` ... Sb.
00a0	41 69 09 40 95 4d 34 3b 6d c6 14 79 21 80 26 42	Ai .@ .M4; m .y ! .&B
00b0	76 ad 65 56 b9 ad 53 58 19 85 ae 3a 5c 85 2a 64	v .eV . .SX ... : \ . *d
00c0	e2 55 c0 f0 49 b4 db 6e ba 43 cb f0 db 31 ad 4b	.U . .I . .n .C ... 1 .K
00d0	1c dc e8 c4 54 20 38 42 56 b3 eb 69 a2 8a 1a 2d	... T 8B V . .i ...
00e0	8d a5 03 cd 46 b4 a1 22 8f 88 b6 31 07 1b 1c d9	... F ... " ... 1 ...
00f0	ad ac 5b 54 ba 5e 76 c5 70 16 8d 52 6c d1 4c c7	.. [T ^v . p . .Rl .L .
0100	43 1d 42 87 07 3e 61 9a c6 be 31 6a 88 44 69 d7	C .B . .>a . . 1j .Di .
0110	5a 22 a2 c5 23 a7 69 67 31 1c 33 8d d7 5e ba 02	Z" . .# .ig 1 .3 . .^ .
0120	22 d6 91 6b 68 d6 bb 59 ad 74 5a d1 c2 d3 20 d6	" . .kh .Y .tZ ...
0130	11 1f 46 e5 2b 3b 4d 4d c8 dd 91 3a 94 6b 85 37	..F .+ ;MM ... : .k .7
0140	2a d7 6b 6d 36 ea 0d 6a a2 da 4d 70 9a 9f 27 57	* .km6 . .j . .Mp . . 'W
0150	67 66 9a ab b4 92 61 66 f7 42 a4 50 5f ab 36 6d	gf ... af .B .P _ .6m
0160	6a b3 98 35 56 33 dc da 5f 15 cf 49 11 95 d4 4f	j . .5V3 . . _ . .I . .0

Source Port (udp.srcport), 2 bytes

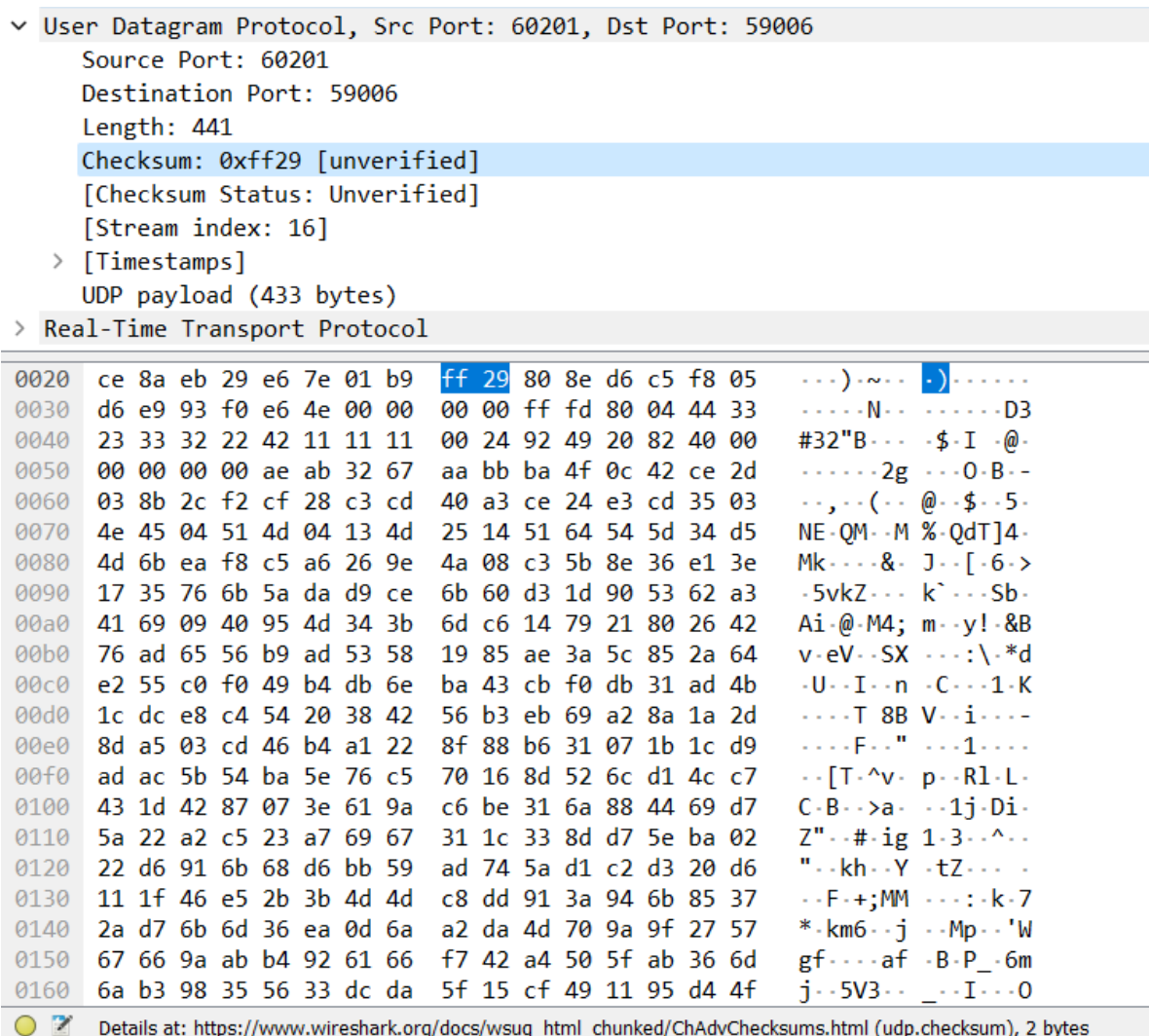
**Hình 2.1.** Độ dài trường Source Port

Source Port: 60201															
Destination Port: 59006															
Length: 441															
Checksum: 0xff29 [unverified]															
[Checksum Status: Unverified]															
[Stream index: 16]															
> [Timestamps]															
UDP payload (433 bytes)															
Real-Time Transport Protocol															
020	ce	8a	eb	29	e6	7e	01	b9	ff	29	80	8e	d6	c5	f8 05
030	d6	e9	93	f0	e6	4e	00	00	00	00	ff	fd	80	04	44 33
040	23	33	32	22	42	11	11	11	00	24	92	49	20	82	40 00
050	00	00	00	00	ae	ab	32	67	aa	bb	ba	4f	0c	42	ce 2d
060	03	8b	2c	f2	cf	28	c3	cd	40	a3	ce	24	e3	cd	35 03
070	4e	45	04	51	4d	04	13	4d	25	14	51	64	54	5d	34 d5
080	4d	6b	ea	f8	c5	a6	26	9e	4a	08	c3	5b	8e	36	e1 3e
090	17	35	76	6b	5a	da	d9	ce	6b	60	d3	1d	90	53	62 a3
0a0	41	69	09	40	95	4d	34	3b	6d	c6	14	79	21	80	26 42
0b0	76	ad	65	56	b9	ad	53	58	19	85	ae	3a	5c	85	2a 64
0c0	e2	55	c0	f0	49	b4	db	6e	ba	43	cb	f0	db	31	ad 4b
0d0	1c	dc	e8	c4	54	20	38	42	56	b3	eb	69	a2	8a	1a 2d
0e0	8d	a5	03	cd	46	b4	a1	22	8f	88	b6	31	07	1b	1c d9
0f0	ad	ac	5b	54	ba	5e	76	c5	70	16	8d	52	6c	d1	4c c7
100	43	1d	42	87	07	3e	61	9a	c6	be	31	6a	88	44	69 d7
110	5a	22	a2	c5	23	a7	69	67	31	1c	33	8d	d7	5e	ba 02
120	22	d6	91	6b	68	d6	bb	59	ad	74	5a	d1	c2	d3	20 d6
130	11	1f	46	e5	2b	3b	4d	4d	c8	dd	91	3a	94	6b	85 37
140	2a	d7	6b	6d	36	ea	0d	6a	a2	da	4d	70	9a	9f	27 57
150	67	66	9a	ab	b4	92	61	66	f7	42	a4	50	5f	ab	36 6d
160	6a	b3	98	35	56	33	dc	da	5f	15	cf	49	11	95	d4 4f
Destination Port (udp.dstport), 2 bytes															

**Hình 2.2.** Độ dài trường Destination Port



**Hình 2.3.** Độ dài trường Length



## Hình 2.4. Độ dài trường Checksum

**Câu 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 tổng độ dài của 8 bytes UDP header và UDP payload

Length 441 bytes = 8 bytes (UDP header) + 433 bytes (Data Payload)

```
✓ User Datagram Protocol, Src Port: 60201, Dst Port: 59006
  Source Port: 60201
  Destination Port: 59006
  Length: 441
  Checksum: 0xff29 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 16]
  > [Timestamps]
  UDP payload (433 bytes)
```

**Hình 3.** Giá trị trường Length

**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?**

Giá trị lớn nhất mà UDP payload có thể có là  $2^{16} - 1$  (do giá trị lưu trong 16 bit) trừ đi 8 bytes header. Bằng  $65535 - 8 = 65527$  bytes.

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

Giá trị lớn nhất mà port nguồn có thể có là  $2^{16} - 1 = 65535$  bytes.

**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. Gợi ý: Có thể bắt gói tin UDP ở một tình huống khác để tìm được 1 cặp gói tin như trên.**

Trong quá trình gửi yêu cầu, IP nguồn gửi Request sẽ trở thành Điểm đích và Source Port sẽ trở thành Destination Port. IP của người gửi Response sẽ trở thành IP nguồn.

66	12.675...	192.168.206.138	192.168.206.140	RTP	46 Unknown RTP version 3
72	12.707...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54981, Time=4161132265, Mark
73	12.733...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54982, Time=4161134616, Mark
74	12.733...	192.168.206.140	192.168.206.138	RTP	178 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36355, Time=4161118800, Mark
76	12.759...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54983, Time=4161136967, Mark
77	12.764...	192.168.206.140	192.168.206.138	RTP	903 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36356, Time=4161133815, Mark
78	12.775...	192.168.206.140	192.168.206.138	RTP	324 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36357, Time=4161127809, Mark
79	12.778...	192.168.206.140	192.168.206.138	RTP	214 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36358, Time=4161124806, Mark
80	12.784...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54984, Time=4161139318, Mark
81	12.786...	192.168.206.140	192.168.206.138	RTP	154 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36359, Time=4161130812, Mark
82	12.802...	192.168.206.140	192.168.206.138	RTP	688 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36360, Time=4161145827, Mark

> Frame 66: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
 > Ethernet II, Src: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65), Dst: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42)  
 > Internet Protocol Version 4, Src: 192.168.206.138, Dst: 192.168.206.140  
 v User Datagram Protocol, Src Port: 59006, Dst Port: 60201

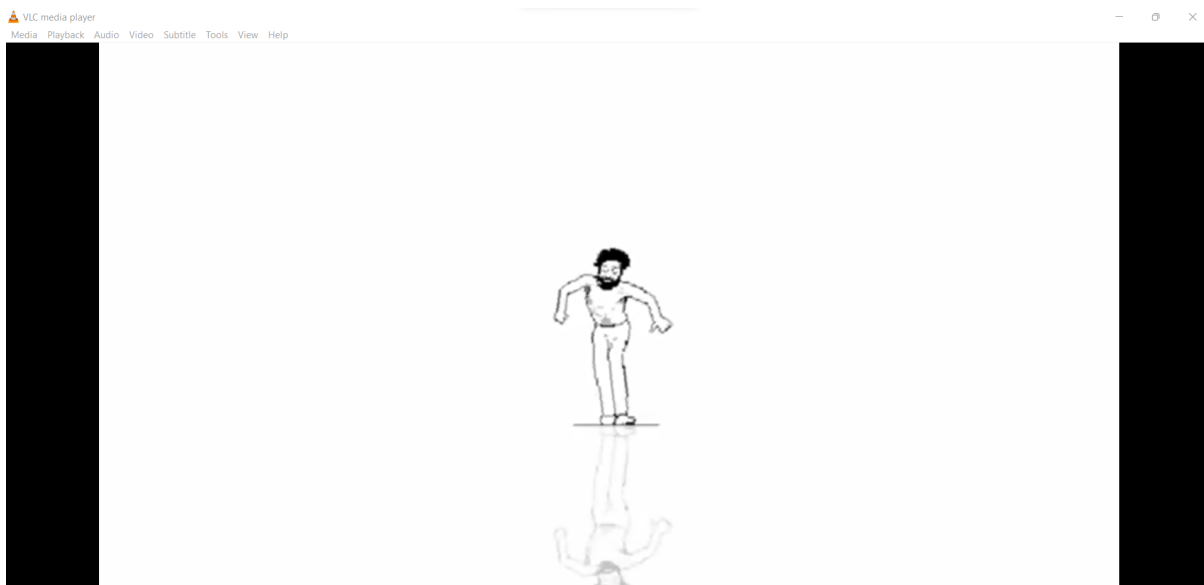
**Hình 6.1.** IP, Port của source và destination.

72	12.707...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54981, Time=4161132265, Mark
73	12.733...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54982, Time=4161134616, Mark
74	12.733...	192.168.206.140	192.168.206.138	RTP	178 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36355, Time=4161118800, Mark
76	12.759...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54983, Time=4161136967, Mark
77	12.764...	192.168.206.140	192.168.206.138	RTP	903 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36356, Time=4161133815, Mark
78	12.775...	192.168.206.140	192.168.206.138	RTP	324 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36357, Time=4161127809, Mark
79	12.778...	192.168.206.140	192.168.206.138	RTP	214 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36358, Time=4161124806, Mark
80	12.784...	192.168.206.140	192.168.206.138	RTP	475 PT=MPEG-I/II Audio, SSRC=0x93F0E64E, Seq=54984, Time=4161139318, Mark
81	12.786...	192.168.206.140	192.168.206.138	RTP	154 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36359, Time=4161130812, Mark
82	12.802...	192.168.206.140	192.168.206.138	RTP	688 PT=DynamicRTP-Type-96, SSRC=0x332DA17, Seq=36360, Time=4161145827, Mark

> Frame 72: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
 > Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)  
 > Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138  
 v User Datagram Protocol, Src Port: 60201, Dst Port: 59006

**Hình 6.2.** IP, Port của source và destination

Hình stream video HTTP.



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

IP của client: 192.168.206.138



TCP Port của client: 52771

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=1 Win=509 Len=0
2	0.009460	192.168.206.140	192.168.206.138	TCP	634	8080 → 52771 [PSH, ACK] Seq=1 Ack=1 Win=4099 Len=580
3	0.016377	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52771 [ACK] Seq=581 Ack=1 Win=4099 Len=1460
4	0.016377	192.168.206.140	192.168.206.138	TCP	596	8080 → 52771 [PSH, ACK] Seq=2041 Ack=1 Win=4099 Len=542
5	0.016484	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=2583 Win=513 Len=0
6	0.020465	192.168.206.140	192.168.206.138	TCP	1030	8080 → 52771 [PSH, ACK] Seq=2583 Ack=1 Win=4099 Len=976
7	0.020558	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=3559 Win=509 Len=0
8	0.067064	192.168.206.140	192.168.206.138	TCP	713	8080 → 52771 [PSH, ACK] Seq=3559 Ack=1 Win=4099 Len=659
9	0.067064	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52771 [ACK] Seq=4218 Ack=1 Win=4099 Len=1460
10	0.067064	192.168.206.140	192.168.206.138	TCP	852	8080 → 52771 [PSH, ACK] Seq=5678 Ack=1 Win=4099 Len=798
11	0.067173	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=6476 Win=513 Len=0
13	0.222282	192.168.206.140	192.168.206.138	TCP	610	8080 → 52771 [PSH, ACK] Seq=6476 Ack=1 Win=4099 Len=556
15	0.262101	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52771 [ACK] Seq=7032 Ack=1 Win=4099 Len=1460
16	0.262101	192.168.206.140	192.168.206.138	TCP	521	8080 → 52771 [PSH, ACK] Seq=8492 Ack=1 Win=4099 Len=467

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
> Ethernet II, Src: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65), Dst: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42)  
> Internet Protocol Version 4, Src: 192.168.206.138, Dst: 192.168.206.140  
> Transmission Control Protocol, Src Port: 52771, Dst Port: 8080, Seq: 1, Ack: 1, Len: 0

Hình 7. IP và TCP Port của client

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

IP của server: 192.168.206.140

TCP Port của server: 8080

1	0.000000	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=1 Win=509 Len=0
2	0.009460	192.168.206.140	192.168.206.138	TCP	634	8080 → 52771 [PSH, ACK] Seq=1 Ack=1 Win=4099 Len=580
3	0.016377	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52771 [ACK] Seq=581 Ack=1 Win=4099 Len=1460
4	0.016377	192.168.206.140	192.168.206.138	TCP	596	8080 → 52771 [PSH, ACK] Seq=2041 Ack=1 Win=4099 Len=542
5	0.016484	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=2583 Win=513 Len=0
6	0.020465	192.168.206.140	192.168.206.138	TCP	1030	8080 → 52771 [PSH, ACK] Seq=2583 Ack=1 Win=4099 Len=976
7	0.020558	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=3559 Win=509 Len=0
8	0.067064	192.168.206.140	192.168.206.138	TCP	713	8080 → 52771 [PSH, ACK] Seq=3559 Ack=1 Win=4099 Len=659
9	0.067064	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52771 [ACK] Seq=4218 Ack=1 Win=4099 Len=1460
10	0.067064	192.168.206.140	192.168.206.138	TCP	852	8080 → 52771 [PSH, ACK] Seq=5678 Ack=1 Win=4099 Len=798
11	0.067173	192.168.206.138	192.168.206.140	TCP	54	52771 → 8080 [ACK] Seq=1 Ack=6476 Win=513 Len=0
13	0.222282	192.168.206.140	192.168.206.138	TCP	610	8080 → 52771 [PSH, ACK] Seq=6476 Ack=1 Win=4099 Len=556
15	0.262101	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52771 [ACK] Seq=7032 Ack=1 Win=4099 Len=1460
16	0.262101	192.168.206.140	192.168.206.138	TCP	521	8080 → 52771 [PSH, ACK] Seq=8492 Ack=1 Win=4099 Len=467

> Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
> Ethernet II, Src: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65), Dst: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42)  
> Internet Protocol Version 4, Src: 192.168.206.138, Dst: 192.168.206.140  
> Transmission Control Protocol, Src Port: 52771, Dst Port: 8080, Seq: 1, Ack: 1, Len: 0

Hình 8. IP và TCP Port của server

**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? Gợi ý: Quan sát trường Flags**

TCP SYN segment có sequence number = 0 để khởi tạo kết nối TCP giữa client và server. (Hình 9.1.)

Trường Flags cờ SYN được set = 1 thì đó là TCP SYN segment (Hình 9.2.)

378	7.831938	192.168.206.138	20.141.10.208	TCP	66	52780 → 443	[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
379	7.853524	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=1 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]
380	7.853524	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=1441 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]
381	7.853524	192.168.206.138	13.107.21.200	TLSv1.2	403		Application Data
382	7.854143	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=3230 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]
383	7.854143	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=3230 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]

> Frame 378: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0

> Ethernet II, Src: LiteonFe\_ac:b1:65 (e8:d0:fc:ac:b1:65), Dst: HP\_b7:76:ef (e8:d8:d1:b7:76:ef)

> Internet Protocol Version 4, Src: 192.168.206.138, Dst: 20.141.10.208

> Transmission Control Protocol, Src Port: 52780, Dst Port: 443, Seq: 0, Len: 0

Hình 9.1. TCP SYN segment

378	7.831938	192.168.206.138	20.141.10.208	TCP	66	52780 → 443	[SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
379	7.853524	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=1 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]
380	7.853524	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=1441 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]
381	7.853524	192.168.206.138	13.107.21.200	TLSv1.2	403		Application Data
382	7.854143	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=3230 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]
383	7.854143	192.168.206.138	13.107.21.200	TCP	1494	52773 → 443	[ACK] Seq=3230 Ack=1 Win=1022 Len=1440 [TCP segment of a reassembled PDU]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

1000 .... = Header Length: 32 bytes (8)

▼ Flags: 0x002 (SYN)

000. .... = Reserved: Not set

...0 .... = Nonce: Not set

....0... .... = Congestion Window Reduced (CWR): Not set

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

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

....0... .... = Acknowledgment: Not set

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

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

> ....0... ..1. = Syn: Set

....0... .... = Fin: Not set

[TCP Flags: .....S.]

Window: 65535

[Calculated window size: 65535]

Hình 9.2. Trường Flags

**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?**

Sequence number của gói SYN/ACK segment = 0.

Giá trị của Acknowledgement trong SYN/ACK segment = 1.

Ta biết segment đó là SYN/ACK segment dựa vào thông tin trong trường Flags (Hình 10.2)



```

991 12.359... 192.168.206.138 13.107.3.254 TCP 66 52783 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
992 12.364... 13.107.3.254 192.168.206.138 TCP 66 443 → 52783 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
993 12.365... 192.168.206.138 13.107.3.254 TCP 54 52783 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
994 12.365... 192.168.206.138 13.107.3.254 TLSv1.2 562 Client Hello
995 12.369... 13.107.3.254 192.168.206.138 TCP 60 443 → 52783 [ACK] Seq=1 Ack=509 Win=4194304 Len=0
996 12.369... 13.107.3.254 192.168.206.138 TLSv1.2 204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
997 12.370... 192.168.206.138 13.107.3.254 TCP 54 52783 → 443 [ACK] Seq=509 Ack=151 Win=261888 Len=0
998 12.370... 192.168.206.138 13.107.3.254 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
999 12.371... 192.168.206.138 13.107.3.254 TLSv1.2 141 Application Data
10... 12.371... 192.168.206.138 13.107.3.254 TLSv1.2 377 Application Data
10 12.374 13.107.3.254 192.168.206.138 TCP 60 443 → 52783 [ACK] Seq=151 Ack=560 Win=4194304 Len=0

> Frame 992: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0
> Ethernet II, Src: HP_b7:76:ef (e8:d8:d1:b7:76:ef), Dst: LiteonTe_ac:b1:65 (e8:d0:fc:ac:b1:65)
> Internet Protocol Version 4, Src: 13.107.3.254, Dst: 192.168.206.138
< Transmission Control Protocol, Src Port: 443, Dst Port: 52783, Seq: 0, Ack: 1, Len: 0
  Source Port: 443
  Destination Port: 52783
  [Stream index: 11]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 0]
  Sequence Number: 0 (relative sequence number)
  Sequence Number (raw): 1271934972
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2715077191
  1000 .... = Header Length: 32 bytes (8)
  < Flags: 0x012 (SYN, ACK)

```

**Hình 10.1.** Gói tin SYN/ACK segment.

```

991 12.359... 192.168.206.138 13.107.3.254 TCP 66 52783 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
992 12.364... 13.107.3.254 192.168.206.138 TCP 66 443 → 52783 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
993 12.365... 192.168.206.138 13.107.3.254 TCP 54 52783 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
994 12.365... 192.168.206.138 13.107.3.254 TLSv1.2 562 Client Hello
995 12.369... 13.107.3.254 192.168.206.138 TCP 60 443 → 52783 [ACK] Seq=1 Ack=509 Win=4194304 Len=0
996 12.369... 13.107.3.254 192.168.206.138 TLSv1.2 204 Server Hello, Change Cipher Spec, Encrypted Handshake Message
997 12.370... 192.168.206.138 13.107.3.254 TCP 54 52783 → 443 [ACK] Seq=509 Ack=151 Win=261888 Len=0
998 12.370... 192.168.206.138 13.107.3.254 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
999 12.371... 192.168.206.138 13.107.3.254 TLSv1.2 141 Application Data
10... 12.371... 192.168.206.138 13.107.3.254 TLSv1.2 377 Application Data
10 12.374 13.107.3.254 192.168.206.138 TCP 60 443 → 52783 [ACK] Seq=151 Ack=560 Win=4194304 Len=0

Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2715077191
1000 .... = Header Length: 32 bytes (8)
< Flags: 0x012 (SYN, ACK)
  000. .... = Reserved: Not set
  ...0 .... = Nonce: Not set
  ....0... = Congestion Window Reduced (CWR): 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.]

```

**Hình 10.2.** Thông tin xác định giá trị Acknowledgement trong trường Flags.

**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?

6 segments đầu tiên mà server gửi cho Client: 2175, 2179, 2200, 2201, 2202, 2203

Sequence number của 6 segments đầu tiên đó là: 1, 104, 503, 1963, 3423, 4883, 5404

21...	37.258...	192.168.206.140	192.168.206.138	TCP	157	8080 → 52786 [PSH, ACK] Seq=1 Ack=143 Win=1049344 Len=103 [TCP segment of a reassembled PDU]
21...	37.280...	192.168.206.138	52.163.231.110	TLSv1.2	112	Application Data
21...	37.311...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080 [ACK] Seq=143 Ack=104 Win=131072 Len=0
21...	37.345...	52.163.231.110	192.168.206.138	TLSv1.2	101	Application Data
21...	37.358...	192.168.206.140	192.168.206.138	TCP	453	8080 → 52786 [PSH, ACK] Seq=104 Ack=143 Win=1049344 Len=399 [TCP segment of a reassembled PDU]
21...	37.387...	192.168.206.138	52.163.231.110	TCP	54	51606 → 443 [ACK] Seq=59 Ack=48 Win=514 Len=0
21...	37.403...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080 [ACK] Seq=143 Ack=503 Win=130816 Len=0
21...	37.467...	192.168.206.138	20.198.119.143	TLSv1.2	98	Application Data
21...	37.556...	20.198.119.143	192.168.206.138	TLSv1.2	229	Application Data

> Frame 2175: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
> Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)  
> Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138  
✓ Transmission Control Protocol, Src Port: 8080, Dst Port: 52786, Seq: 1, Ack: 143, Len: 103  
Source Port: 8080  
Destination Port: 52786  
[Stream index: 16]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 103]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 4005634038  
[Next Sequence Number: 104 (relative sequence number)]  
Acknowledgment Number: 143 (relative ack number)  
Acknowledgment number (raw): 2727944230  
0101 .... = Header Length: 20 bytes (5)

Hình 11.1. Segment 1

21...	37.358...	192.168.206.140	192.168.206.138	TCP	453	8080 → 52786 [PSH, ACK] Seq=104 Ack=143 Win=1049344 Len=399 [TCP segment of a reassembled PDU]
21...	37.387...	192.168.206.138	52.163.231.110	TCP	54	51606 → 443 [ACK] Seq=59 Ack=48 Win=514 Len=0
21...	37.403...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080 [ACK] Seq=143 Ack=503 Win=130816 Len=0
21...	37.467...	192.168.206.138	20.198.119.143	TLSv1.2	98	Application Data
21...	37.556...	20.198.119.143	192.168.206.138	TLSv1.2	229	Application Data

> Frame 2179: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
> Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)  
> Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138  
✓ Transmission Control Protocol, Src Port: 8080, Dst Port: 52786, Seq: 104, Ack: 143, Len: 399  
Source Port: 8080  
Destination Port: 52786  
[Stream index: 16]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 399]  
Sequence Number: 104 (relative sequence number)  
Sequence Number (raw): 4005634141  
[Next Sequence Number: 503 (relative sequence number)]  
Acknowledgment Number: 143 (relative ack number)  
Acknowledgment number (raw): 2727944230  
0101 .... = Header Length: 20 bytes (5)

Hình 11.2. Segment 2

22...	45.394...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786 [ACK] Seq=503 Ack=143 Win=1049344 Len=1460 [TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786 [ACK] Seq=1963 Ack=143 Win=1049344 Len=1460 [TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786 [ACK] Seq=3423 Ack=143 Win=1049344 Len=1460 [TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	575	8080 → 52786 [PSH, ACK] Seq=4883 Ack=143 Win=1049344 Len=521 [TCP segment of a reassembled PDU]

> Frame 2200: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0  
> Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)  
> Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138  
✓ Transmission Control Protocol, Src Port: 8080, Dst Port: 52786, Seq: 503, Ack: 143, Len: 1460  
Source Port: 8080  
Destination Port: 52786  
[Stream index: 16]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 1460]  
Sequence Number: 503 (relative sequence number)  
Sequence Number (raw): 4005634540  
[Next Sequence Number: 1963 (relative sequence number)]  
Acknowledgment Number: 143 (relative ack number)  
Acknowledgment number (raw): 2727944230  
0101 .... = Header Length: 20 bytes (5)

Hình 11.3. Segment 3

22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=1963	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=3423	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	575	8080 → 52786	[PSH, ACK]	Seq=4883	Ack=143	Win=1049344	Len=521	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=5404	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	300	8080 → 52786	[PSH, ACK]	Seq=6864	Ack=143	Win=1049344	Len=246	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=7110	Win=131328	Len=0	
22...	45.468...	192.168.206.140	192.168.206.138	TCP	713	8080 → 52786	[PSH, ACK]	Seq=7110	Ack=143	Win=1049344	Len=659	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=7769	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=9229	Win=131328	Len=0	
22...	45.507...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=9229	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.140	192.168.206.138	TCP	705	8080 → 52786	[PSH, ACK]	Seq=10689	Ack=143	Win=1049344	Len=651	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=11340	Win=131328	Len=0	

> Frame 2201: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0

> Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)

> Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138

> Transmission Control Protocol, Src Port: 8080, Dst Port: 52786, Seq: 1963, Ack: 143, Len: 1460

Source Port: 8080

Destination Port: 52786

[Stream index: 16]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 1460]

Sequence Number: 1963 (relative sequence number)

Sequence Number (raw): 4005636000

[Next Sequence Number: 3423 (relative sequence number)]

Acknowledgment Number: 143 (relative ack number)

Acknowledgment number (raw): 2727944230

0101 .... = Header Length: 20 bytes (5)

## Hình 11.4. Segment 4

22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=3423	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	575	8080 → 52786	[PSH, ACK]	Seq=4883	Ack=143	Win=1049344	Len=521	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=5404	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	300	8080 → 52786	[PSH, ACK]	Seq=6864	Ack=143	Win=1049344	Len=246	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=7110	Win=131328	Len=0	
22...	45.468...	192.168.206.140	192.168.206.138	TCP	713	8080 → 52786	[PSH, ACK]	Seq=7110	Ack=143	Win=1049344	Len=659	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=7769	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=9229	Win=131328	Len=0	
22...	45.507...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=9229	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.140	192.168.206.138	TCP	705	8080 → 52786	[PSH, ACK]	Seq=10689	Ack=143	Win=1049344	Len=651	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=11340	Win=131328	Len=0	

> Frame 2202: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0

> Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)

> Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138

> Transmission Control Protocol, Src Port: 8080, Dst Port: 52786, Seq: 3423, Ack: 143, Len: 1460

Source Port: 8080

Destination Port: 52786

[Stream index: 16]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 1460]

Sequence Number: 3423 (relative sequence number)

Sequence Number (raw): 4005637460

[Next Sequence Number: 4883 (relative sequence number)]

Acknowledgment Number: 143 (relative ack number)

Acknowledgment number (raw): 2727944230

0101 .... = Header Length: 20 bytes (5)

## Hình 11.5. Segment 5

22...	45.410...	192.168.206.140	192.168.206.138	TCP	575	8080 → 52786	[PSH, ACK]	Seq=4883	Ack=143	Win=1049344	Len=521	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=5404	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.140	192.168.206.138	TCP	300	8080 → 52786	[PSH, ACK]	Seq=6864	Ack=143	Win=1049344	Len=246	[TCP segment of a reassembled PDU]
22...	45.410...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=7110	Win=131328	Len=0	
22...	45.468...	192.168.206.140	192.168.206.138	TCP	713	8080 → 52786	[PSH, ACK]	Seq=7110	Ack=143	Win=1049344	Len=659	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=7769	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=9229	Win=131328	Len=0	
22...	45.507...	192.168.206.140	192.168.206.138	TCP	1514	8080 → 52786	[ACK]	Seq=9229	Ack=143	Win=1049344	Len=1460	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.140	192.168.206.138	TCP	705	8080 → 52786	[PSH, ACK]	Seq=10689	Ack=143	Win=1049344	Len=651	[TCP segment of a reassembled PDU]
22...	45.507...	192.168.206.138	192.168.206.140	TCP	54	52786 → 8080	[ACK]	Seq=143	Ack=11340	Win=131328	Len=0	

> Frame 2203: 575 bytes on wire (4600 bits), 575 bytes captured (4600 bits) on interface \Device\NPF\_{5E9DD202-E175-468A-A1D7-0048ECA3526E}, id 0

> Ethernet II, Src: IntelCor\_5d:f6:42 (88:d8:2e:5d:f6:42), Dst: LiteonTe\_ac:b1:65 (e8:d0:fc:ac:b1:65)

> Internet Protocol Version 4, Src: 192.168.206.140, Dst: 192.168.206.138

> Transmission Control Protocol, Src Port: 8080, Dst Port: 52786, Seq: 4883, Ack: 143, Len: 521

Source Port: 8080

Destination Port: 52786

[Stream index: 16]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 521]

Sequence Number: 4883 (relative sequence number)

Sequence Number (raw): 4005638920

[Next Sequence Number: 5404 (relative sequence number)]

Acknowledgment Number: 143 (relative ack number)

Acknowledgment number (raw): 2727944230

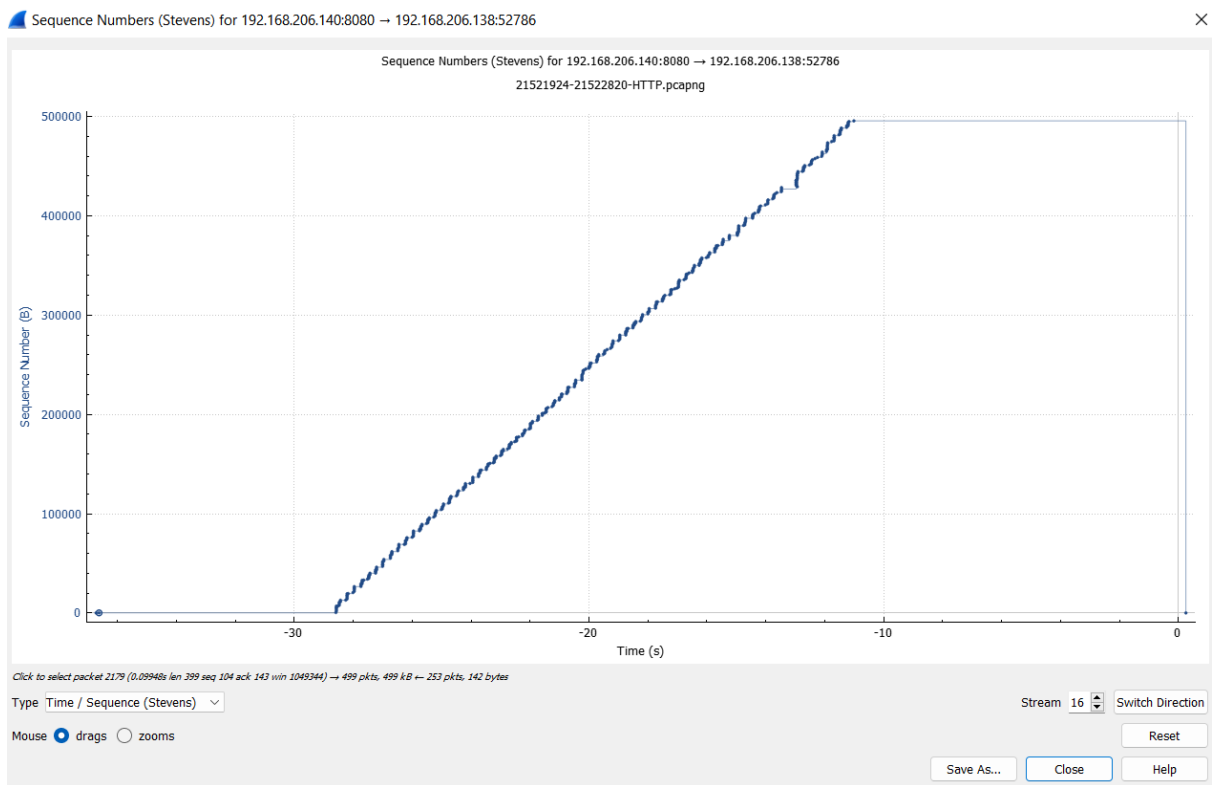
0101 .... = Header Length: 20 bytes (5)

## Hình 11.6. Segment 6

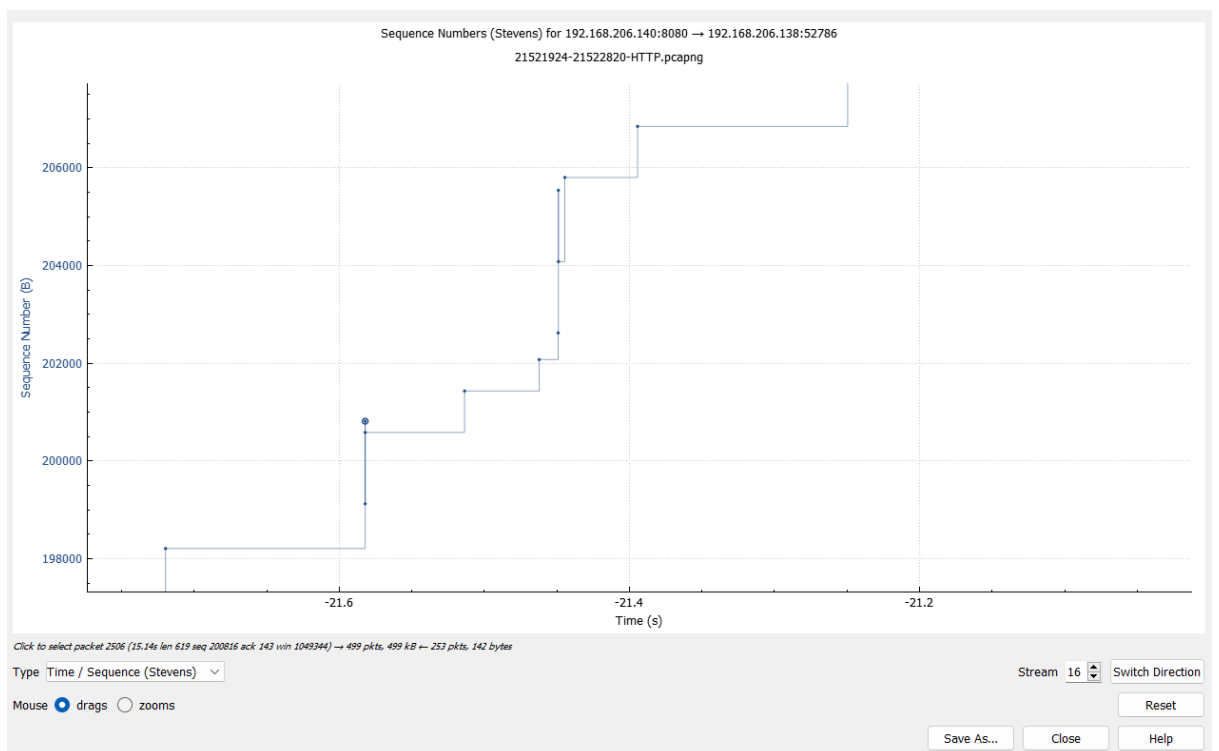
STT	Thời gian gửi	Thời gian nhận	RTT (Round Trip Time)
1	37.258542	37.311407	0.052865
2	37.358020	37.403721	0.045701
3	45.394749	45.401157	0.006408
4	45.410041	45.507667	0.097626
5	45.410041	45.507965	0.097924
6	45.410041	45.548675	0.138634

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

Dựa vào sequence number và biểu đồ dưới, ta tìm thấy các gói cùng sequence number ở các thời điểm khác nhau => Có segment gửi lại



**Hình 12.1.** Biểu đồ Sequence Number



**Hình 12.2.** Biểu đồ Sequence Number khi đã phóng to