

BÁO CÁO THỰC HÀNH

Môn học: Nhập môn Mạng Máy tính

Tên chủ đề: Phân tích hoạt động giao thức TCP - UDP

GVHD: Tô Trọng Nghĩa

THÔNG TIN CHUNG:

Lớp: IT005.0119.2

STT	Họ và tên	MSSV	Email
1	Nguyễn Trọng Nhân	22521005	22521005@gm.uit.edu.vn

1. NỘI DUNG THỰC HIỆN:¹

STT	Nội dung	Tình trạng	Trang
1	Phân tích hoạt động giao thức UDP	100%	2 – 5
2	Phân tích hoạt động giao thức TCP	100%	5 – 10
Điểm tự đánh giá			10/10

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

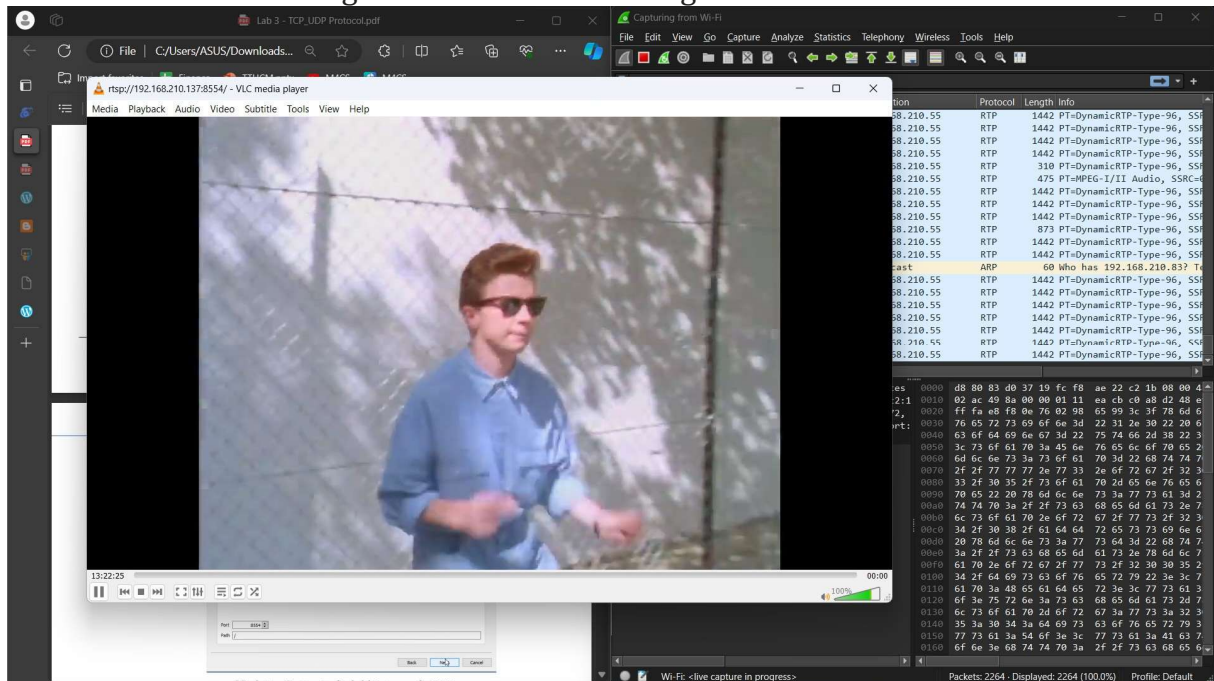
¹ Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Task 1: Phân tích hoạt động giao thức UDP

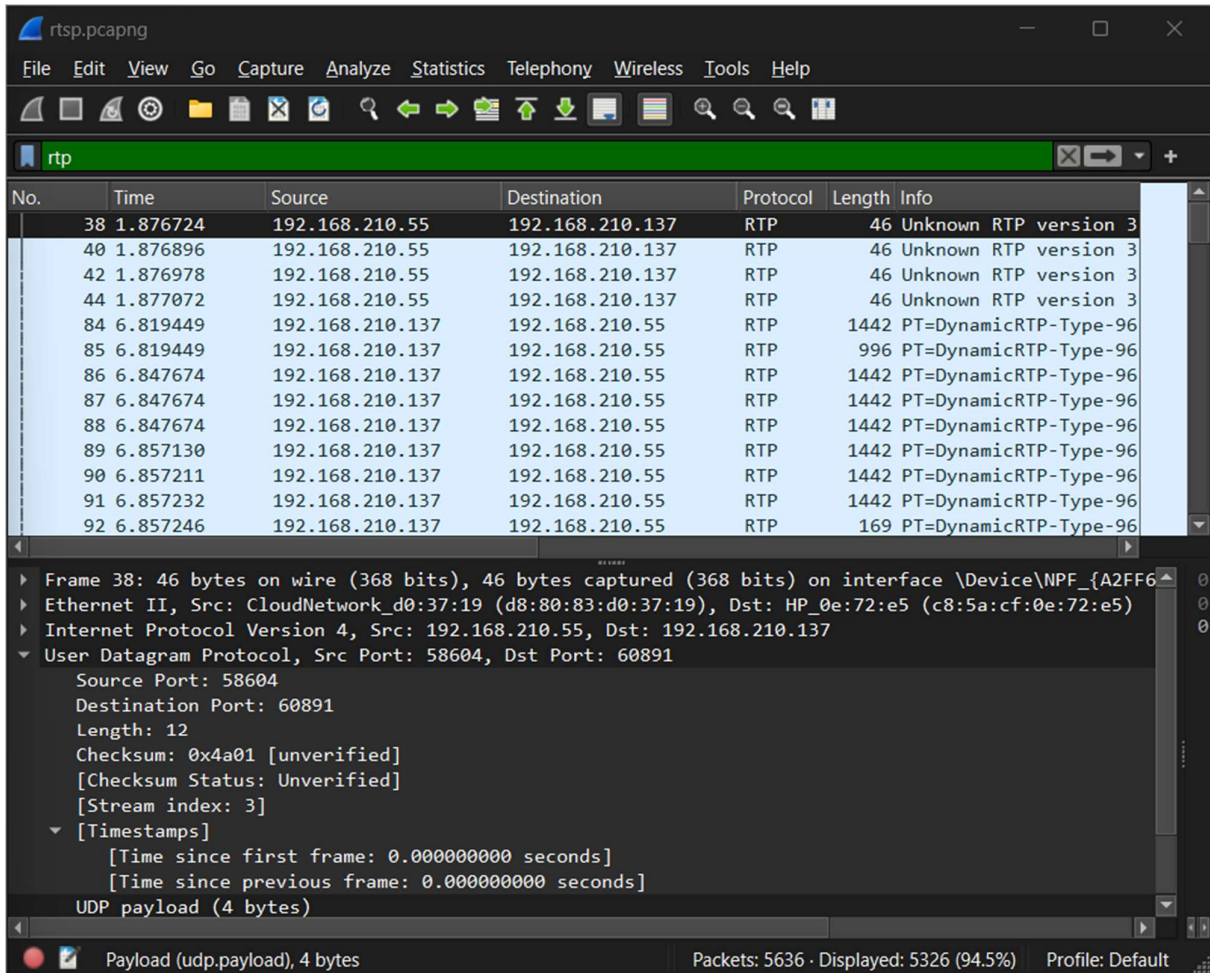
1.1 Streaming video sử dụng UDP

1.2 Tiến hành bắt gói tin UDP khi streaming video



1.3 Phân tích hoạt động giao thức UDP

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.



No.	Time	Source	Destination	Protocol	Length	Info
38	1.876724	192.168.210.55	192.168.210.137	RTP	46	Unknown RTP version 3
40	1.876896	192.168.210.55	192.168.210.137	RTP	46	Unknown RTP version 3
42	1.876978	192.168.210.55	192.168.210.137	RTP	46	Unknown RTP version 3
44	1.877072	192.168.210.55	192.168.210.137	RTP	46	Unknown RTP version 3
84	6.819449	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
85	6.819449	192.168.210.137	192.168.210.55	RTP	996	PT=DynamicRTP-Type-96
86	6.847674	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
87	6.847674	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
88	6.847674	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
89	6.857130	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
90	6.857211	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
91	6.857232	192.168.210.137	192.168.210.55	RTP	1442	PT=DynamicRTP-Type-96
92	6.857246	192.168.210.137	192.168.210.55	RTP	169	PT=DynamicRTP-Type-96

Frame 38: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{A2FF6...}

Ethernet II, Src: CloudNetwork_d0:37:19 (d8:80:83:d0:37:19), Dst: HP_0e:72:e5 (c8:5a:cf:0e:72:e5)

Internet Protocol Version 4, Src: 192.168.210.55, Dst: 192.168.210.137

User Datagram Protocol, Src Port: 58604, Dst Port: 60891

Source Port: 58604
Destination Port: 60891
Length: 12
Checksum: 0x4a01 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Timestamps]
[Time since first frame: 0.00000000 seconds]
[Time since previous frame: 0.00000000 seconds]
UDP payload (4 bytes)

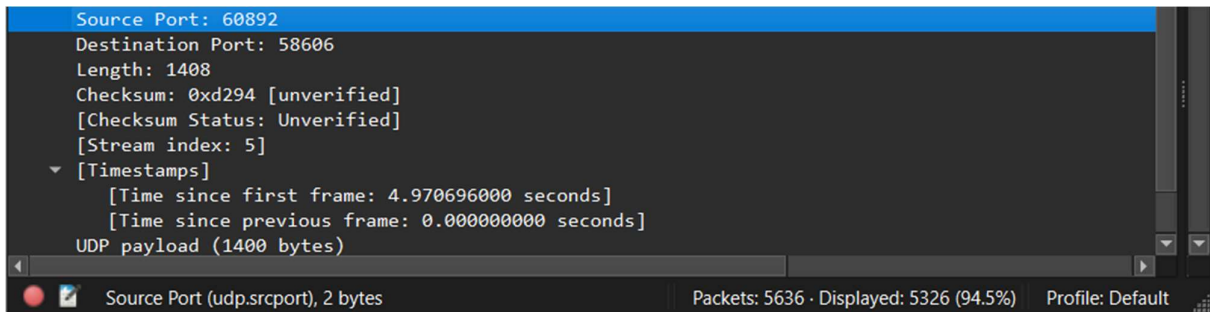
Payload (udp.payload), 4 bytes

Packets: 5636 · Displayed: 5326 (94.5%) Profile: Default

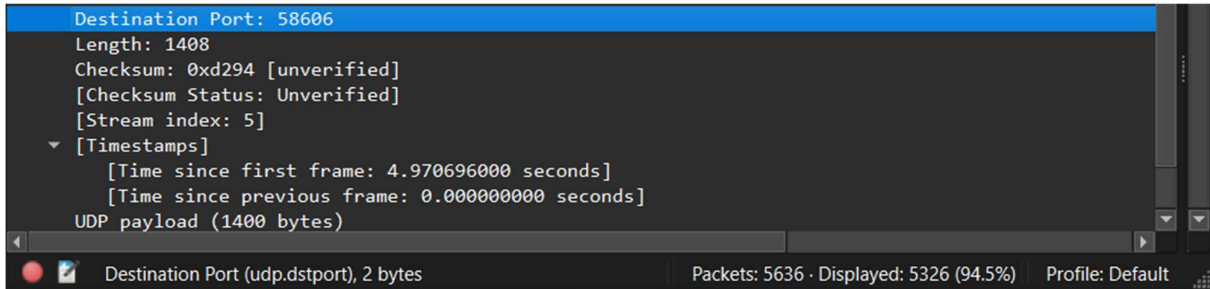
Các trường có trong UDP header gồm:

- Source port: Trường này xác định cổng của người gửi thông tin và có ý nghĩa nếu muốn nhận thông tin phản hồi từ người nhận.
- Destination port: Trường xác định cổng nhận thông tin, và trường này là cần thiết.
- Length: Trường có độ dài 16 bit xác định chiều dài của toàn bộ datagram: phần header và dữ liệu. Chiều dài tối thiểu là 8 byte khi gói tin không có dữ liệu, chỉ có header.
- Checksum: Trường checksum 16 bit dùng cho việc kiểm tra lỗi của phần header và dữ liệu.

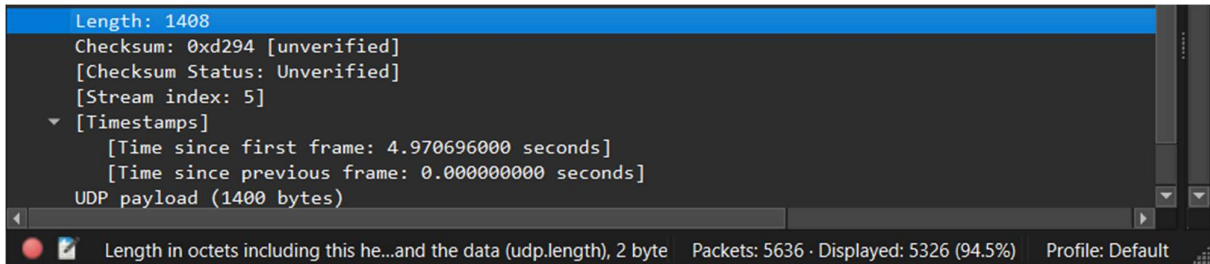
2. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?



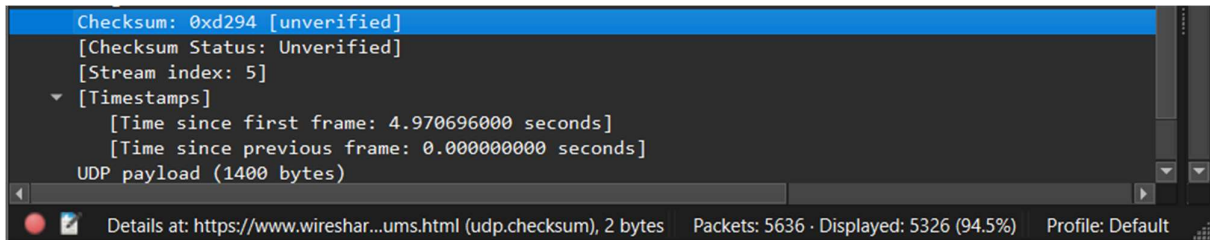
Source port: 2 bytes



Destination port: 2 bytes



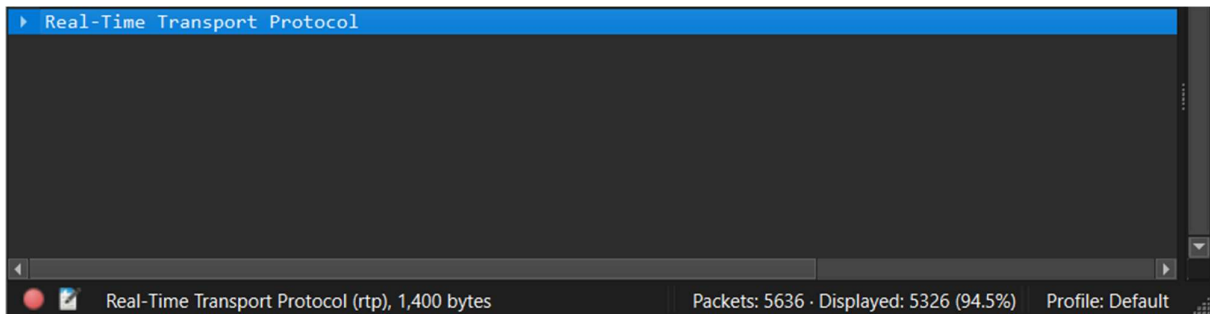
Length: 2 bytes



Checksum: 2 bytes

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

Giá trị trường Length trong UDP header là độ dài của toàn bộ datagram, gồm header và data.



Data: 1400 bytes

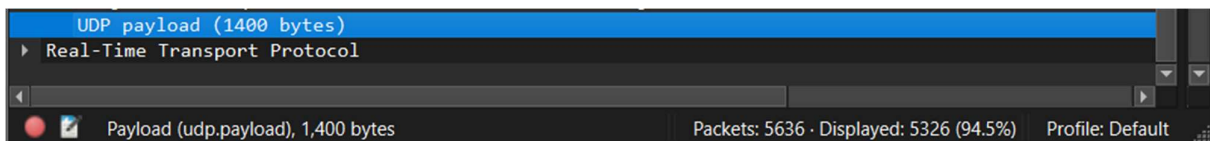
Header: 8 bytes

Length: 1408

Length: 1408 bytes

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

1400 bytes



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

Do có 2 bytes -> 16 bits -> $2^{16}-1 = 65535$

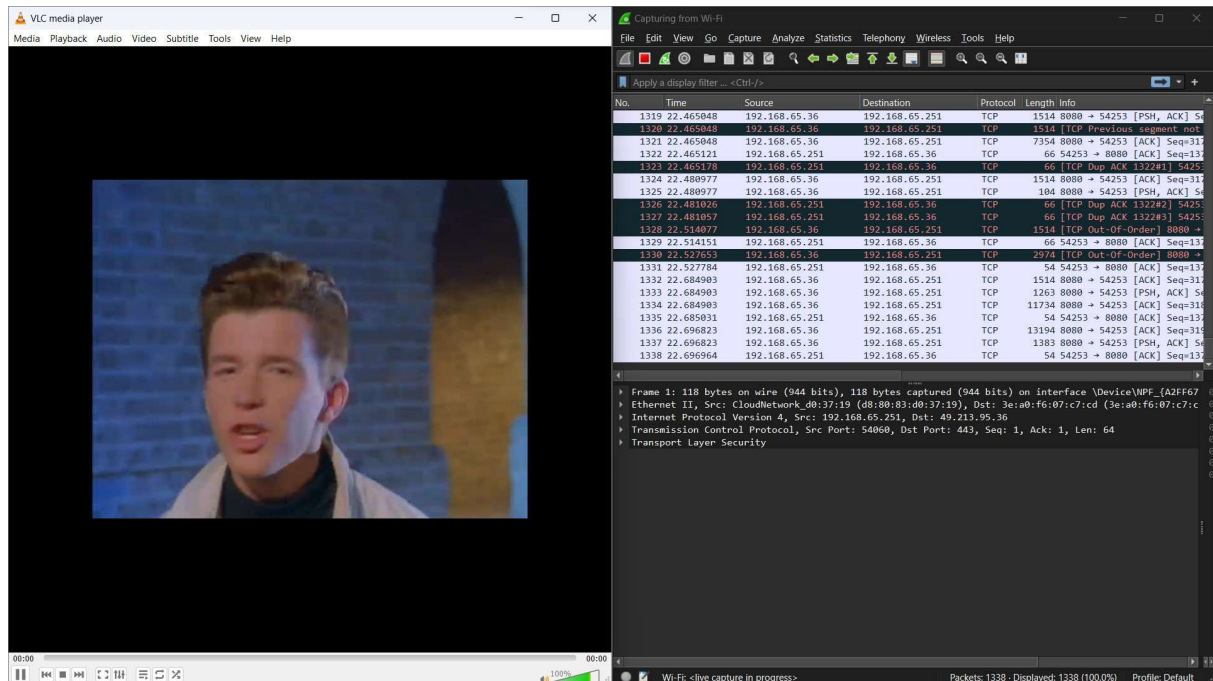
6. * Tìm và kiểm tra một cặp gói tin sử dụng giao thức UDP gồm: gói tin do máy mình gửi và gói tin phản hồi của gói tin đó. Miêu tả mối quan hệ về port number của 2 gói tin này.

46	2.400164	172.67.163.103	192.168.65.251	UDP	1242	443 → 54165	Len=1200
48	2.427853	192.168.65.251	172.67.163.103	UDP	87	54165 → 443	Len=45

Các port number tương ứng với ip, không đổi.

2. Task 2: Phân tích hoạt động giao thức TCP

2.1 Streaming video sử dụng HTTP và bắt gói tin TCP



2.2 Phân tích hoạt động giao thức TCP

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

9	1.450211	192.168.65.251	192.168.65.36	HTTP	190 GET / HTTP/1.
---	----------	----------------	---------------	------	-------------------

IP client: 192.168.65.251

6	1.386815	192.168.65.251	192.168.65.36	TCP	66 54253 → 8080
---	----------	----------------	---------------	-----	-----------------

TCP port: 54253

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

9	1.450211	192.168.65.251	192.168.65.36	HTTP	190 GET / HTTP/1.
---	----------	----------------	---------------	------	-------------------

IP server: 192.168.65.36

6	1.386815	192.168.65.251	192.168.65.36	TCP	66 54253 → 8080
---	----------	----------------	---------------	-----	-----------------

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 of a TCP connection. The packet list at the top shows a series of packets, with packet 9 highlighted in yellow. Packet 9 is an HTTP GET request from 192.168.65.251 to 192.168.65.36 on port 8080. The packet details pane below shows the structure of the selected packet, including the Internet Protocol Version 4 header, the Transmission Control Protocol header, and the HTTP request body. The TCP header shows the source port as 54253, the destination port as 8080, and the flags set to SYN (0x002). The sequence number is 0 (relative sequence number), and the acknowledgment number is 0. The window size is 64240. The packet length is 190 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.65.251	49.213.95.36	TLSv1.2	118	Application D
2	0.080158	49.213.95.36	192.168.65.251	TCP	54	443 → 54060 [
3	0.090328	49.213.95.36	192.168.65.251	TLSv1.2	114	Application D
4	0.133739	192.168.65.251	49.213.95.36	TCP	54	54060 → 443 [
6	1.386815	192.168.65.251	192.168.65.36	TCP	66	54253 → 8080
7	1.449399	192.168.65.36	192.168.65.251	TCP	66	8080 → 54253
8	1.449532	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080
9	1.450211	192.168.65.251	192.168.65.36	HTTP	190	GET / HTTP/1.
10	1.483086	192.168.65.36	192.168.65.251	TCP	157	8080 → 54253
11	1.537045	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080
12	1.552274	192.168.65.36	192.168.65.251	TCP	452	8080 → 54253
13	1.593504	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080
14	2.794783	192.168.65.36	192.168.65.251	TCP	11734	8080 → 54253
15	2.794875	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080
16	2.812132	192.168.65.36	192.168.65.251	TCP	2974	8080 → 54253
17	2.812202	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080
18	2.828962	192.168.65.36	192.168.65.251	TCP	1514	8080 → 54253
19	2.828962	192.168.65.36	192.168.65.251	TCP	17574	8080 → 54253
20	2.829060	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080
21	2.830426	192.168.65.36	192.168.65.251	TCP	10274	8080 → 54253
22	2.830482	192.168.65.251	192.168.65.36	TCP	54	54253 → 8080

Internet Protocol Version 4, Src: 192.168.65.251, Dst: 192.168.65.36

Transmission Control Protocol, Src Port: 54253, Dst Port: 8080, Seq: 0, Len: 0

Source Port: 54253
Destination Port: 8080
[Stream index: 1]

[Conversation completeness: Complete, WITH_DATA (47)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1526819500
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1000 = Header Length: 32 bytes (8)

Flags: 0x002 (SYN)
Window: 64240
[Calculated window size: 64240]
Checksum: 0xb683 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation
[Timestamps]

Transmission Control Protocol: Protocol Packets: 3498 · Displayed: 3426 (97.9%) Profile: Default

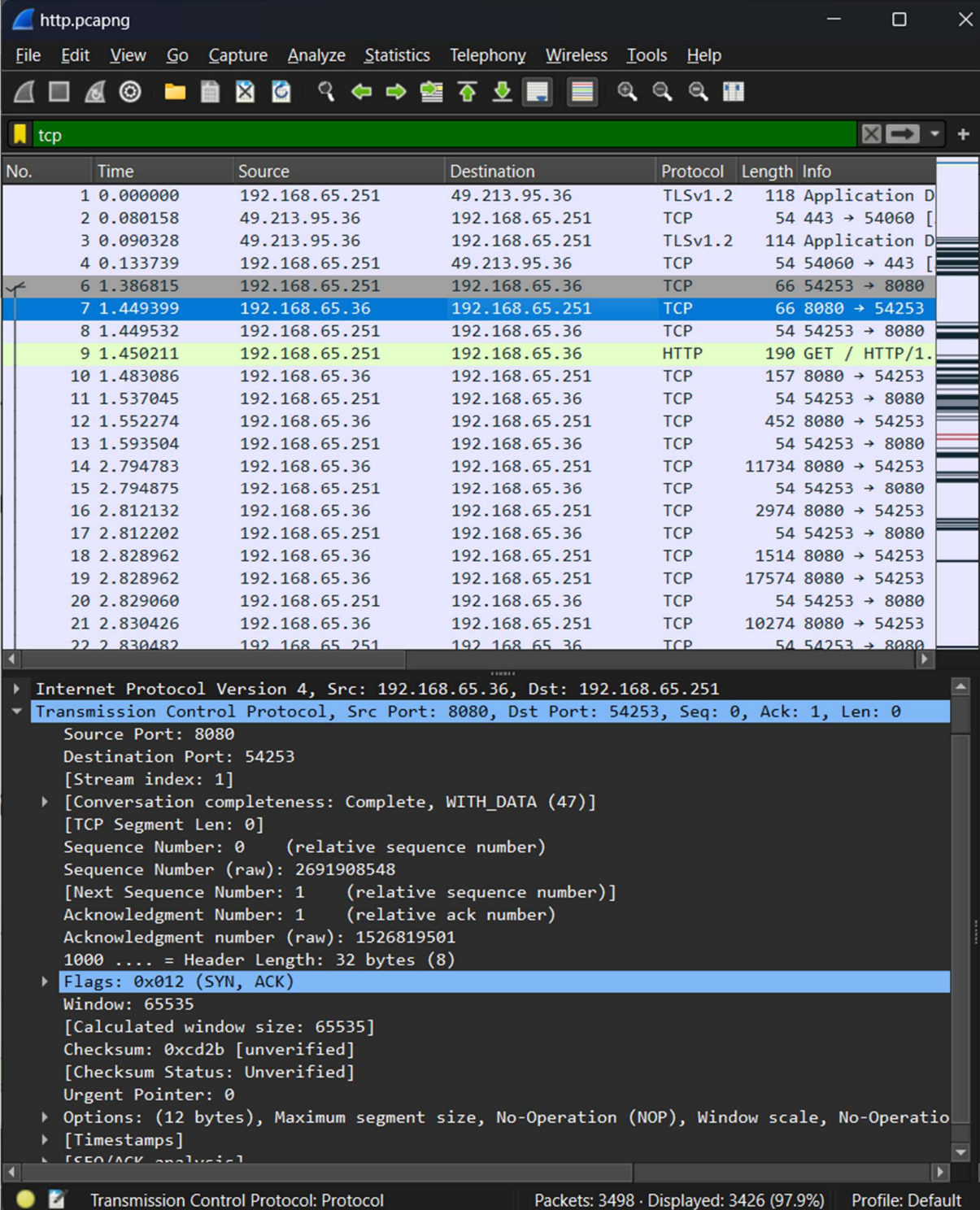
Sequence Number: 0

Thành phần Flags cho biết đây là gói TCP SYN

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?



The image shows a Wireshark packet capture of a network traffic. The packet list at the top shows a series of packets. Packet 7 is highlighted, showing a TCP segment from 192.168.65.36 to 192.168.65.251 with Seq: 0 and Ack: 1. The packet details pane shows the following information:

- Internet Protocol Version 4, Src: 192.168.65.36, Dst: 192.168.65.251
- Transmission Control Protocol, Src Port: 8080, Dst Port: 54253, Seq: 0, Ack: 1, Len: 0
 - Source Port: 8080
 - Destination Port: 54253
 - [Stream index: 1]
 - [Conversation completeness: Complete, WITH_DATA (47)]
 - [TCP Segment Len: 0]
 - Sequence Number: 0 (relative sequence number)
 - Sequence Number (raw): 2691908548
 - [Next Sequence Number: 1 (relative sequence number)]
 - Acknowledgment Number: 1 (relative ack number)
 - Acknowledgment number (raw): 1526819501
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x012 (SYN, ACK)
 - Window: 65535
 - [Calculated window size: 65535]
 - Checksum: 0xcd2b [unverified]
 - [Checksum Status: Unverified]
 - Urgent Pointer: 0
 - Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation
 - [Timestamps]
 - [SYN/ACK analysis]

Sequence Number = 0

Acknowledgement Number = 1

```

▼ 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. ]

```

Bit cờ của trường ACK = 1 và bit cờ trường SYN = 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?

10	1.483086	192.168.65.36	192.168.65.251	TCP	157 8080 → 54253	[PSH, ACK] Seq=1 Ack=137 Win=525312 Len=103 [TCP segment of a reassembled PDU]
12	1.552274	192.168.65.36	192.168.65.251	TCP	452 8080 → 54253	[PSH, ACK] Seq=104 Ack=137 Win=525312 Len=398 [TCP segment of a reassembled PDU]
14	2.794783	192.168.65.36	192.168.65.251	TCP	11734 8080 → 54253	[ACK] Seq=502 Ack=137 Win=525312 Len=11680 [TCP segment of a reassembled PDU]
16	2.812132	192.168.65.36	192.168.65.251	TCP	2974 8080 → 54253	[ACK] Seq=12182 Ack=137 Win=525312 Len=2920 [TCP segment of a reassembled PDU]
18	2.828962	192.168.65.36	192.168.65.251	TCP	1514 8080 → 54253	[ACK] Seq=15102 Ack=137 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
19	2.828962	192.168.65.36	192.168.65.251	TCP	17574 8080 → 54253	[ACK] Seq=16562 Ack=137 Win=525312 Len=17520 [TCP segment of a reassembled PDU]

Sequence Number của 6 gói: 1 – 104 – 502 – 12182 – 15102 – 16562

10	1.483086	192.168.65.36	192.168.65.251	TCP	157 8080 → 54253	[PSH, ACK] Seq=1 Ack=137 Win=525312 Len=103 [TCP segment of a reassembled PDU]
11	1.537045	192.168.65.251	192.168.65.36	TCP	54 54253 → 8080	[ACK] Seq=137 Ack=104 Win=65536 Len=0
12	1.552274	192.168.65.36	192.168.65.251	TCP	452 8080 → 54253	[PSH, ACK] Seq=104 Ack=137 Win=525312 Len=398 [TCP segment of a reassembled PDU]
13	1.593504	192.168.65.251	192.168.65.36	TCP	54 54253 → 8080	[ACK] Seq=137 Ack=502 Win=655024 Len=0
14	2.794783	192.168.65.36	192.168.65.251	TCP	11734 8080 → 54253	[ACK] Seq=502 Ack=137 Win=525312 Len=11680 [TCP segment of a reassembled PDU]
15	2.794875	192.168.65.251	192.168.65.36	TCP	54 54253 → 8080	[ACK] Seq=137 Ack=12182 Win=65536 Len=0
16	2.812132	192.168.65.36	192.168.65.251	TCP	2974 8080 → 54253	[ACK] Seq=12182 Ack=137 Win=525312 Len=2920 [TCP segment of a reassembled PDU]
17	2.812202	192.168.65.251	192.168.65.36	TCP	54 54253 → 8080	[ACK] Seq=137 Ack=15102 Win=65536 Len=0
18	2.828962	192.168.65.36	192.168.65.251	TCP	1514 8080 → 54253	[ACK] Seq=15102 Ack=137 Win=525312 Len=1460 [TCP segment of a reassembled PDU]
19	2.828962	192.168.65.36	192.168.65.251	TCP	17574 8080 → 54253	[ACK] Seq=16562 Ack=137 Win=525312 Len=17520 [TCP segment of a reassembled PDU]
20	2.829060	192.168.65.251	192.168.65.36	TCP	54 54253 → 8080	[ACK] Seq=137 Ack=34082 Win=65536 Len=0

Thời gian các segment được gửi, thời gian ACK và RTT

STT	Thời gian gửi	Thời gian nhận ACK	RTT
10	1.483086	1.537045	0.107918
12	1.552274	1.593504	0.08246
14	2.794783	2.794875	0.000184
16	2.812132	2.812202	0.00014
18	2.828962	Loss	Không có
19	2.828962	2.829060	0.000196

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

Có segment được gửi lại. Thông tin ở đồ thị TCP, mỗi chấm trong biểu đồ tượng trưng cho một TCP segment có sequence number tương ứng với thời gian segment đó được gửi đi. Lưu ý là một chồng các dấu chấm tương ứng với một chuỗi các gói tin được gửi liên tiếp nhau.

