Lab 3

BÁO CÁO BÀI THỰC HÀNH SỐ 3

Giao thức TCP & UDP

LAB 3 – UDP & TCP PROTOCOL

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Mai Nguyễn Nam Phương (22521164)
Thời gian thực hiện	18/10/2023 – 24/10/2023
Tự chấm điểm	10/10

TRẢ LỜI CÁC CÂU HỎI

Câu 1. Điền thông tin vào bảng sau

Trả lời:

IP Address	172.30.220.151
MAC Address	2C-0D-A7-70-24-9D
Default gateway IP address	172.30.0.1
DNS sever IP address	8.8.8.8 8.8.4.4

```
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . . . . . : 2C-0D-A7-70-24-9D
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f9d7:1a7e:5836:1736%17(Preferred)
IPv4 Address. . . . . . . . . . . : 172.30.220.151(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.0.0
Lease Obtained. . . . . . . . . . : Saturday, November 18, 2023 2:01:20 PM
Lease Expires . . . . . . . . . . : Saturday, November 18, 2023 9:00:45 PM
Default Gateway . . . . . . . . . : 172.30.0.1
DHCP Server . . . . . . . . . . . : 192.168.199.13
DHCPv6 IAID . . . . . . . . . . . : 288099751
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2C-91-64-E0-D4-93-90-1C-95-54
DNS Servers . . . . . . . . . . . : 8.8.8.8
                                    8.8.4.4
NetBIOS over Tcpip. . . . . . . . : Enabled
```

Câu 2. Tại danh sách của gói tin bắt được, định vị gói tin truy vấn domain google.com

Trả lời: Dựa vào hình ảnh ta thấy được gói tin truy vấn là gói tin thứ 194 và 201

190	3.353107	172.30.220.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
193	3.411476	8.8.8.8	172.30.220.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
194	3.413612	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
200	3.475642	8.8.8.8	172.30.220.151	DNS	166	Standard query response 0x0002 A google.com A 74.125.68.113 A 74.125.68.138 A 74.125.68.102 A 74.125.68.100 A 74.
201	3.478841	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
202	3.537529	8.8.8.8	172.30.220.151	DNS	182	Standard query response 0x0003 AAAA google.com AAAA 2404:6800:4003:c02::65 AAAA 2404:6800:4003:c02::71 AAAA 2404:

Câu 3. Định vị gói tin phản hồi của truy vấn trên? Từ thông điệp trả lời ghi lại địa chỉ IP của domain google.com

dns

No.	Time	Source	Destination	Protocol	Length	Info
190	3.353107	172.30.220.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
193	3.411476	8.8.8.8	172.30.220.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.google
194	3.413612	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
200	3.475642	8.8.8.8	172.30.220.151	DNS	166	Standard query response 0x0002 A google.com A 74.125.68.113 A 74.125.68.138 A 74.125.68.102 A 74.125.68.100 A 74.125.68.139 A 74.125.68.101
201	3.478841	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
202	3.537529	8.8.8.8	172.30.220.151	DNS	182	Standard query response 0x0003 AAAA google.com AAAA 2404:6800:4003:c02::65 AAAA 2404:6800:4003:c02::71 AAAA 2404:6800:4003:c02::8a AAAA 2404:6800:4003:c02::8b

Trả lời: Ta sẽ thấy được gói tin phản hồi là gói 200 và 202

Từ đó có IP của domain google.com là:

74.125.68.113 A 74.125.68.138 A 74.125.68.102 A 74.125.68.100 A 74.125.68.139 A 74.125.68.101 (IPv4)

2404:6800:4003:c02::65 AAAA 2404:6800:4003:c02::71 AAAA 2404:6800:4003:c02::8a AAAA 2404:6800:4003:c02::8b (IPv6)

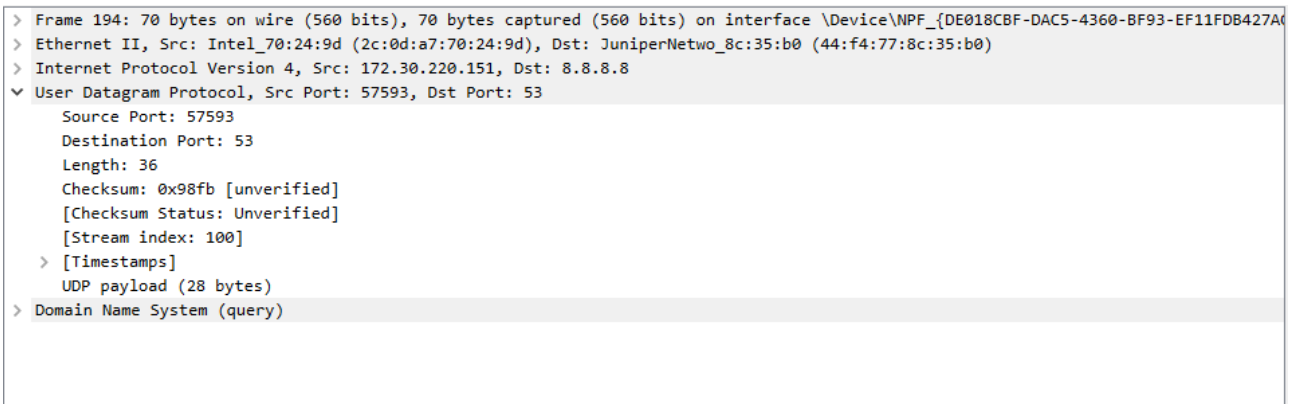
Câu 4. Chọn 1 gói tin DNS, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó

Trả lời: Bao gồm 4 field

Source Port: Port gốc
Destination Port: Port đích
Length: Độ dài gói tin
Checksum: Giá trị kiểm tra

- Giải thích:

+ 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
+ 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. Phương pháp tính checksum được định nghĩa trong RFC 768.



Câu 5. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header

Trả lời:
UDP gồm 4 trường, kích thước mỗi trường:
- Source Port: 2 bytes
- Destination port: 2 bytes
- Length: 2 bytes
- Checksum: 2 bytes

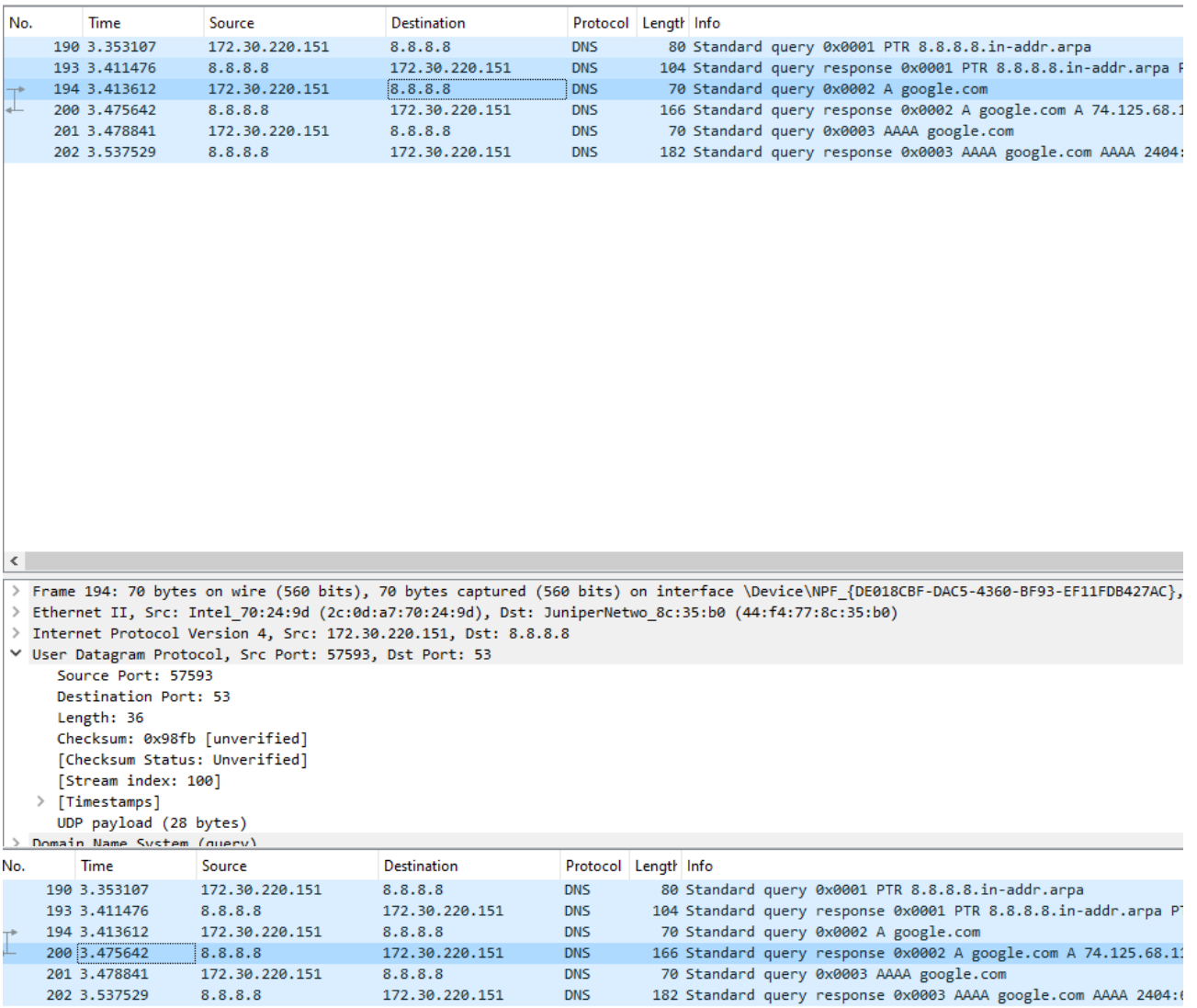
Câu 6. Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này

Trả lời: Giá trị của trường Length là trường chỉ định độ dài tổng cộng của gói UDP, bao gồm cả header và dữ liệu. Trường này đo lường bằng byte và bao gồm độ dài của cả phần header và phần dữ liệu
Ở đây độ dài của gói tin bao gồm 8 bytes header + độ dài data
Length (36) = 8 + data (28)

```
Source Port: 57593
Destination Port: 53
Length: 36
Checksum: 0x98fb [unverified]
[Checksum Status: Unverified]
[Stream index: 100]
[Timestamps]
UDP payload (28 bytes)
```

Câu 7. Quan sát 2 gói tin tìm được ở câu 2 và câu 3, mô tả mối quan hệ giữa các địa chỉ IP và port number của 2 gói tin này

Trả lời: Trong quá trình gửi yêu cầu, IP nguồn gửi Request sẽ trở thành điểm đích và Source Port sẽ trở thành Destination Port. IP người gửi Respone sẽ trở thành IP nguồn hay có thể hiểu là các giá trị IP và Port của nguồn và đích sẽ đảo lại với nhau



No.	Time	Source	Destination	Protocol	Length	Info
190	3.353107	172.30.220.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
193	3.411476	8.8.8.8	172.30.220.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa P
194	3.413612	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
200	3.475642	8.8.8.8	172.30.220.151	DNS	166	Standard query response 0x0002 A google.com A 74.125.68.1
201	3.478841	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
202	3.537529	8.8.8.8	172.30.220.151	DNS	182	Standard query response 0x0003 AAAA google.com AAAA 2404:

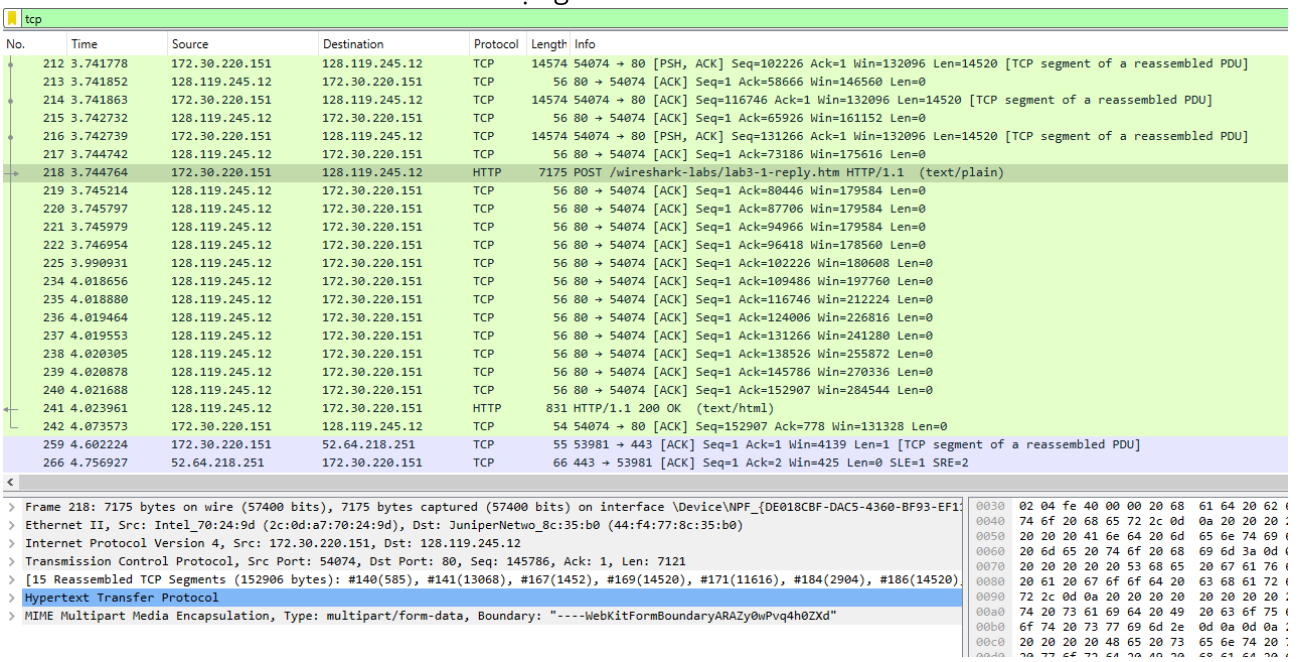
```
> Frame 194: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{DE018CBF-DAC5-4360-BF93-EF11FDB427AC},
> Ethernet II, Src: Intel_70:24:9d (2c:0d:a7:70:24:9d), Dst: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0)
> Internet Protocol Version 4, Src: 172.30.220.151, Dst: 8.8.8.8
v User Datagram Protocol, Src Port: 57593, Dst Port: 53
    Source Port: 57593
    Destination Port: 53
    Length: 36
    Checksum: 0x98fb [unverified]
    [Checksum Status: Unverified]
    [Stream index: 100]
  > [Timestamps]
    UDP payload (28 bytes)
> Domain Name System (query)
```


No.	Time	Source	Destination	Protocol	Length	Info
190	3.353107	172.30.220.151	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
193	3.411476	8.8.8.8	172.30.220.151	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa P
194	3.413612	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0002 A google.com
200	3.475642	8.8.8.8	172.30.220.151	DNS	166	Standard query response 0x0002 A google.com A 74.125.68.1
201	3.478841	172.30.220.151	8.8.8.8	DNS	70	Standard query 0x0003 AAAA google.com
202	3.537529	8.8.8.8	172.30.220.151	DNS	182	Standard query response 0x0003 AAAA google.com AAAA 2404:

```
> Frame 200: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface \Device\NPF_{DE018CBF-DAC5-4360-BF93-EF11FDB427
> Ethernet II, Src: JuniperNetwo_8c:35:b0 (44:f4:77:8c:35:b0), Dst: Intel_70:24:9d (2c:0d:a7:70:24:9d)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.30.220.151
v User Datagram Protocol, Src Port: 53, Dst Port: 57593
    Source Port: 53
    Destination Port: 57593
    Length: 132
    Checksum: 0x111d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 100]
  > [Timestamps]
    UDP payload (124 bytes)
> Domain Name System (response)
```

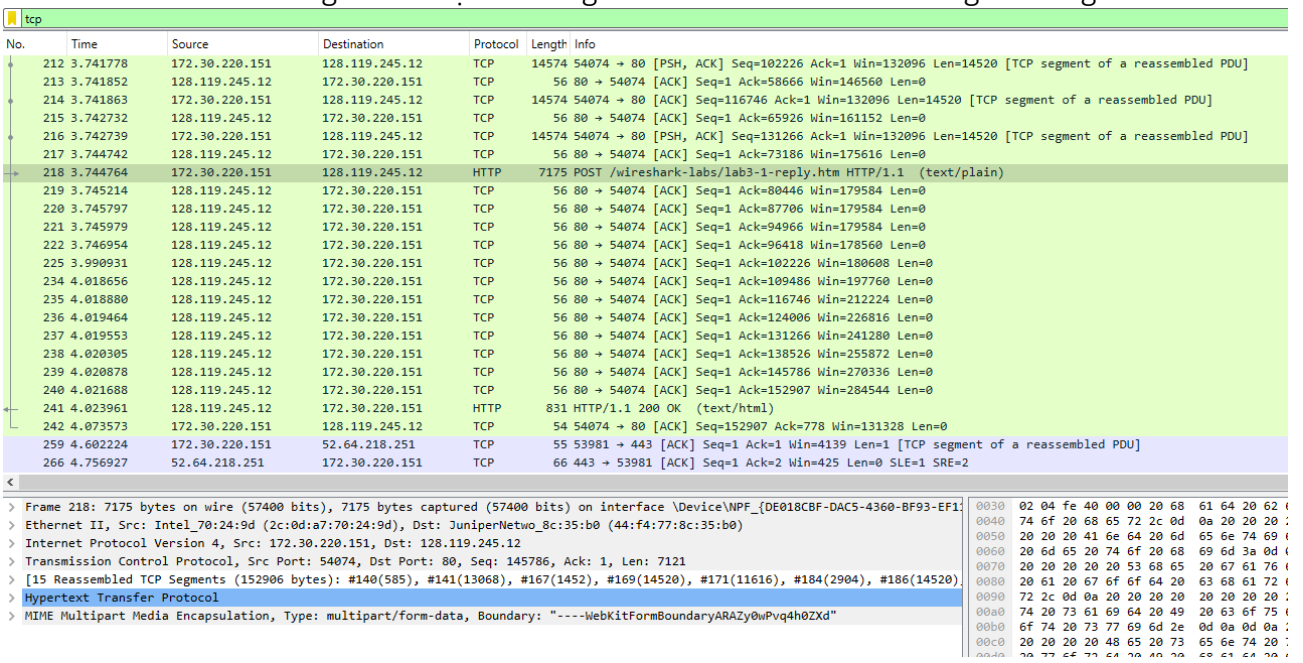
Câu 8. Xác định IP và TCP Port của client sử dụng để chuyển tệp sang gaia.cs.umass.edu là gì?

Trả lời: Dựa trên gợi ý ta chọn vào gói tin thông điệp HTTP là 218 và biết được IP của client là 172.30.220.151 và sử dụng Port 54074



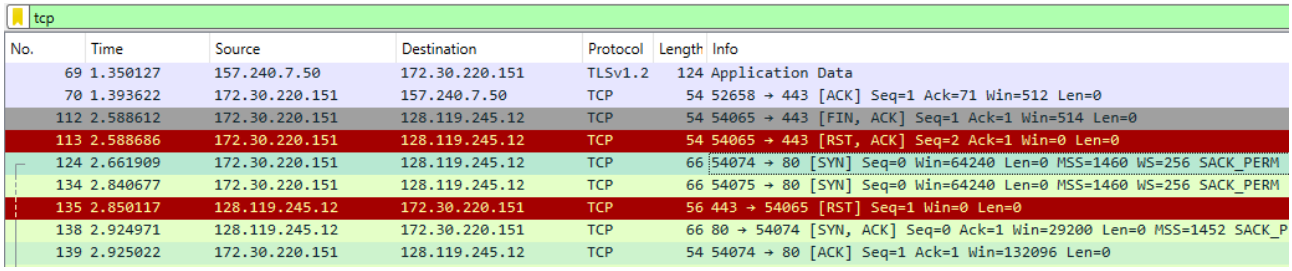
Câu 9. Địa chỉ IP của gaia.cs.umass.edu là gì? Trên số cổng nào nó gửi và nhận các segment TCP cho kết nối này

Trả lời: Tương tự như câu trên thì địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12 và nó gửi và nhận các segment TCP cho kết nối bằng số cổng 80

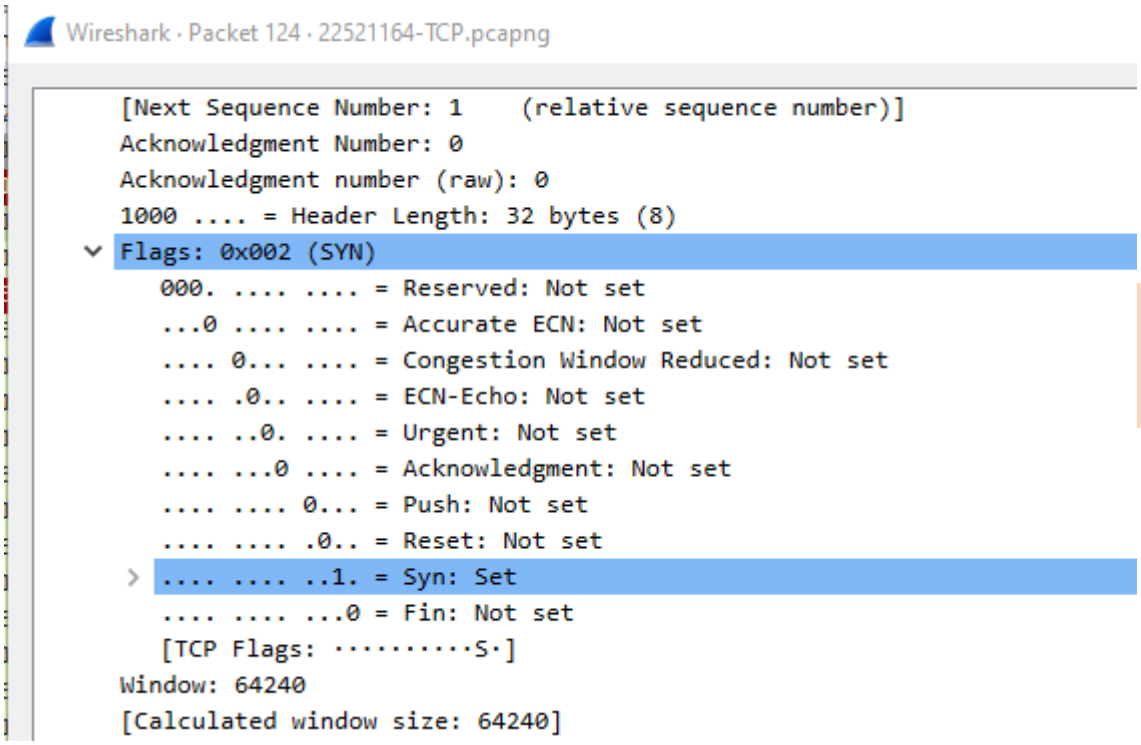


Câu 10. TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment

Trả lời: TCP SYN segment sử dụng sequence number bằng 0 để tạo kết nối TCP giữa client và server



Ta kiểm tra trong trường Flags của gói, nếu cờ SYN được set = 1 thì đó là TCP SYN segment

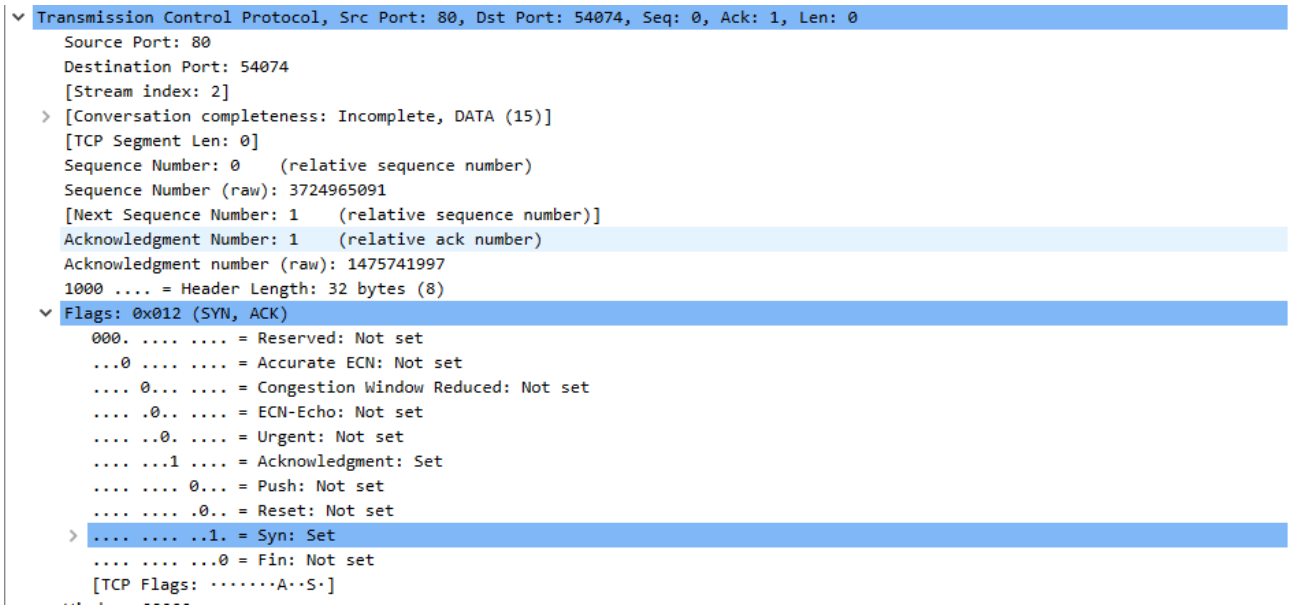


Câu 11. Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment

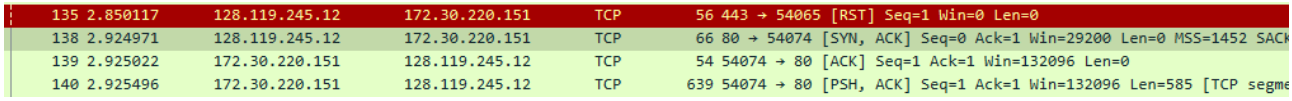
Trả lời: Ta có thể thấy gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment có rất nhiều, ở đây ta lấy ví dụ là gói tin 138 => có thể thấy sequence number của nó là 0

Câu 12. 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?

Trả lời: Giá trị của Acknowledgement trong SYN/ACK segment là 1, server có thể xác định nó nhờ vào thông tin của gói tin và có thể nhận biết nó qua trường Flags trong SYN/ACK segment



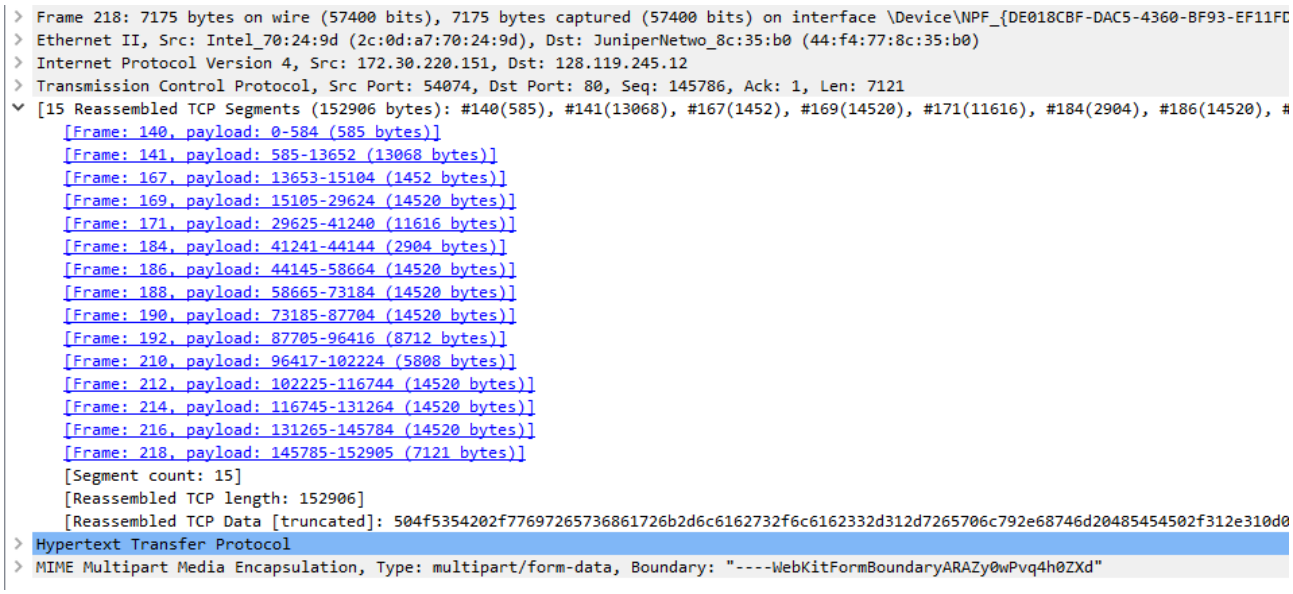
Ta có thể biết segment đó là SYN/ACK segment nhờ vào trường Info của Wireshark

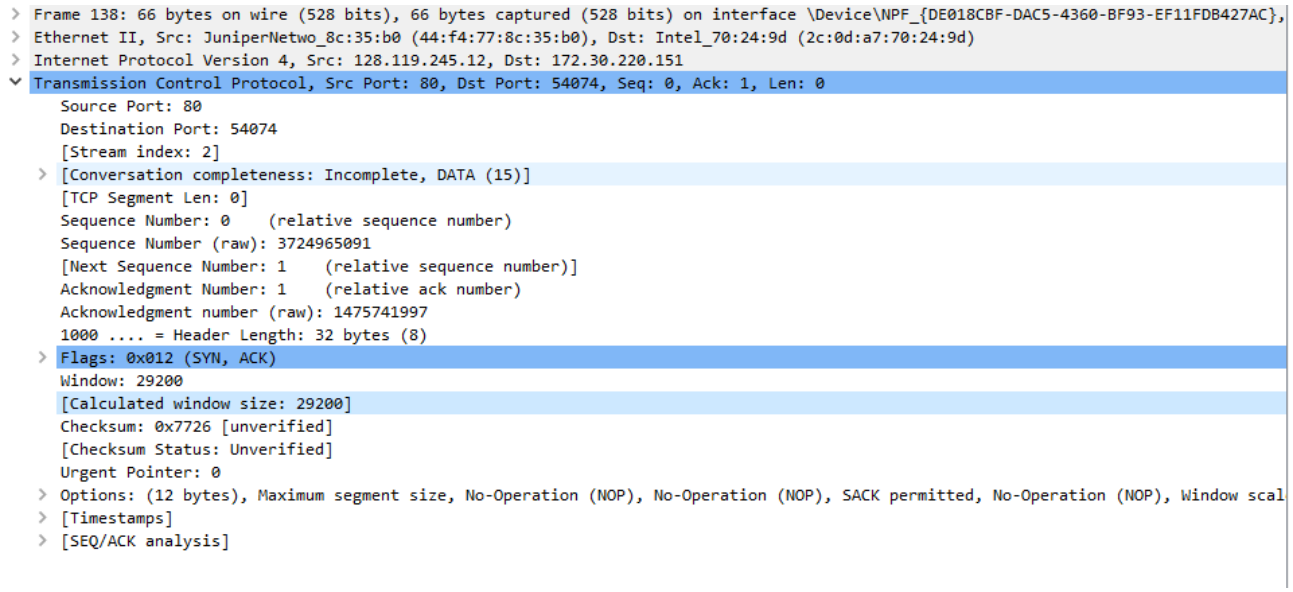


Câu 13. Tìm độ dài của từng segment trong bộ 6 segment đầu tiên trên? Tìm lượng buffer còn trống nhỏ nhất mà bên nhận thông báo cho bên gửi trong suốt truyền tin

Trả lời: 6 segment đầu tiên là 140,141,167,169,171 và 184 với độ dài lần lượt là 585 bytes, 13068 bytes, 1452 bytes, 14520 bytes, 11616 bytes, 2904 bytes

Lượng buffer còn trống nhỏ nhất là 29200

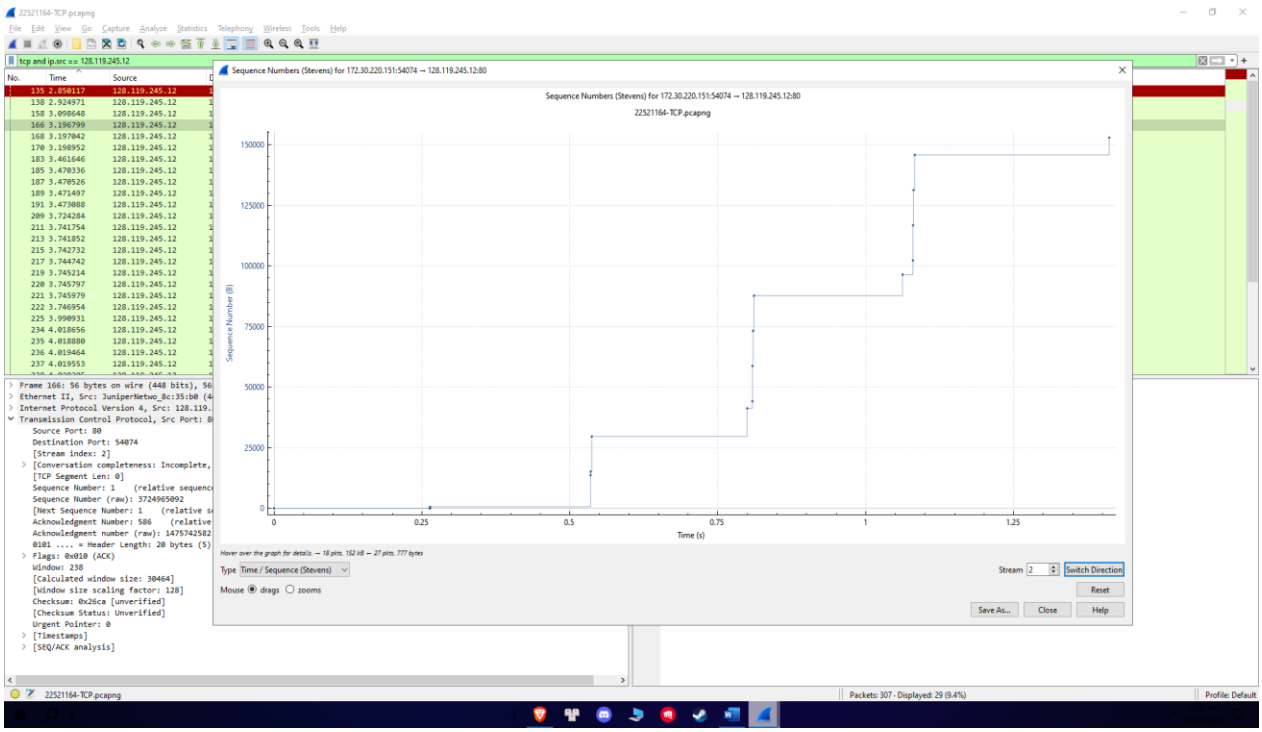




Câu 14. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình truyền tin cho chúng ta biết điều đó?

- Không có segment nào được gửi lại

- Dựa vào biểu đồ phân tích truyền gói tin có thể thấy các gói tin có cùng sequence number ở các thời điểm khác nhau không được tìm thấy


Sequence Numbers (Stevens) for 172.30.220.151:54074 → 128.119.245.12:80
Sequence Numbers (Stevens) for 172.30.220.151:54074 → 128.119.245.12:80
22521164-TCP.pcapng
Sequence Number (B)
Time (s)
Type Time / Sequence (Stevens)
Mouse drags zooms
Stream
Switch Direction
Reset
Save As...
Close
Help