Lab 3

BÁO CÁO BÀI THỰC HÀNH SỐ 3

Phân tích giao thức UDP và TCP

(UDP & TCP Protocol)

Môn học: Nhập môn Mạng máy tính

Giảng viên hướng dẫn	ThS. Đỗ Thị Hương Lan
Sinh viên thực hiện	Nguyễn Duy Khang (22520619)
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	15/11/2023 – 22/11/2023
Tự chấm điểm	9.5/10

A. CÁC BƯỚC THỰC HÀNH

Gợi ý: *Ghi rõ từng bước thực hành, chụp hình ảnh screenshot để báo cáo thêm trực quan*

B. TRẢ LỜI CÁC CÂU HỎI

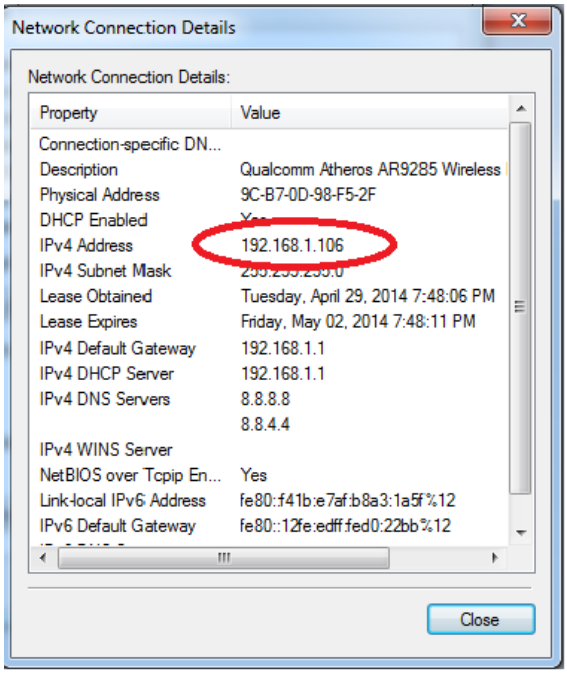
Gợi ý: *Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn*.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

Trả lời: *192.168.1.106*

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



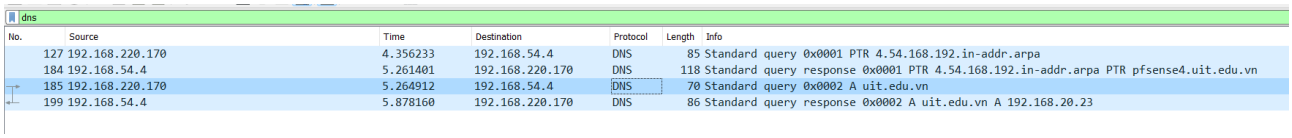
I. Truy vấn DNS

1. Bắt các gói tin truy vấn và phản hồi của DNS

Pv4, Link-local IPv6 address	172.27.160.1 fe80::18eb:a39e:35b5:cddb%47
MAC address	00-15-5D-B4-FF-AD
Default gateway	fe80::1 192.168.220.1
DNS Servers	192.168.54.4 192.168.20.4

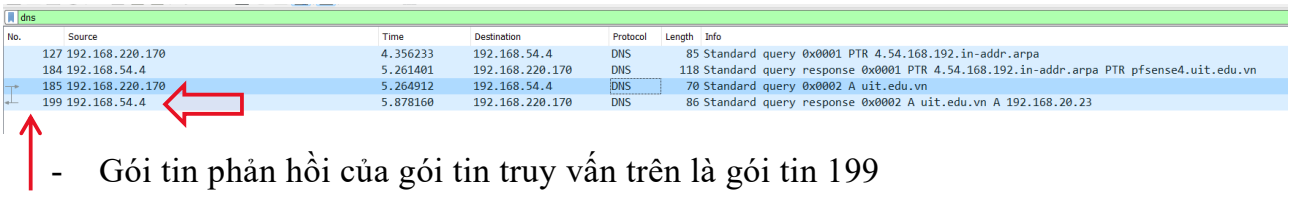
II. Phân tích các gói tin UDP

1. Tại danh sách các gói tin bắt được, định vị gói tin truy vấn domain uit.edu.vn (hoặc domain tự chọn).Gợi ý: chứa "standard query" và "A uit.edu.vn"



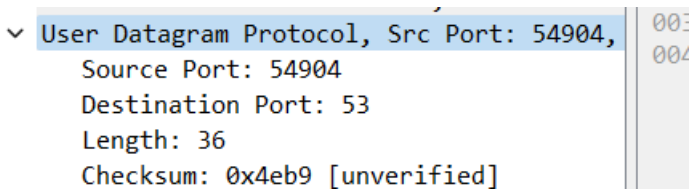
- Quan sát ở trường info, ta quan sát được gói tin truy vấn domain uit.edu.vn là gói tin thứ 185.

2. Xác định gói tin phản hồi của truy vấn trên? Từ thông điệp phản hồi, ghi lại địa chỉ IP của domain uit.edu.vn



- Gói tin phản hồi của gói tin truy vấn trên là gói tin 199
- Quan sát ở trường source trong gói tin phản hồi, ta tìm được địa chỉ IP của domain uit.edu.vn là 192.168.54.4

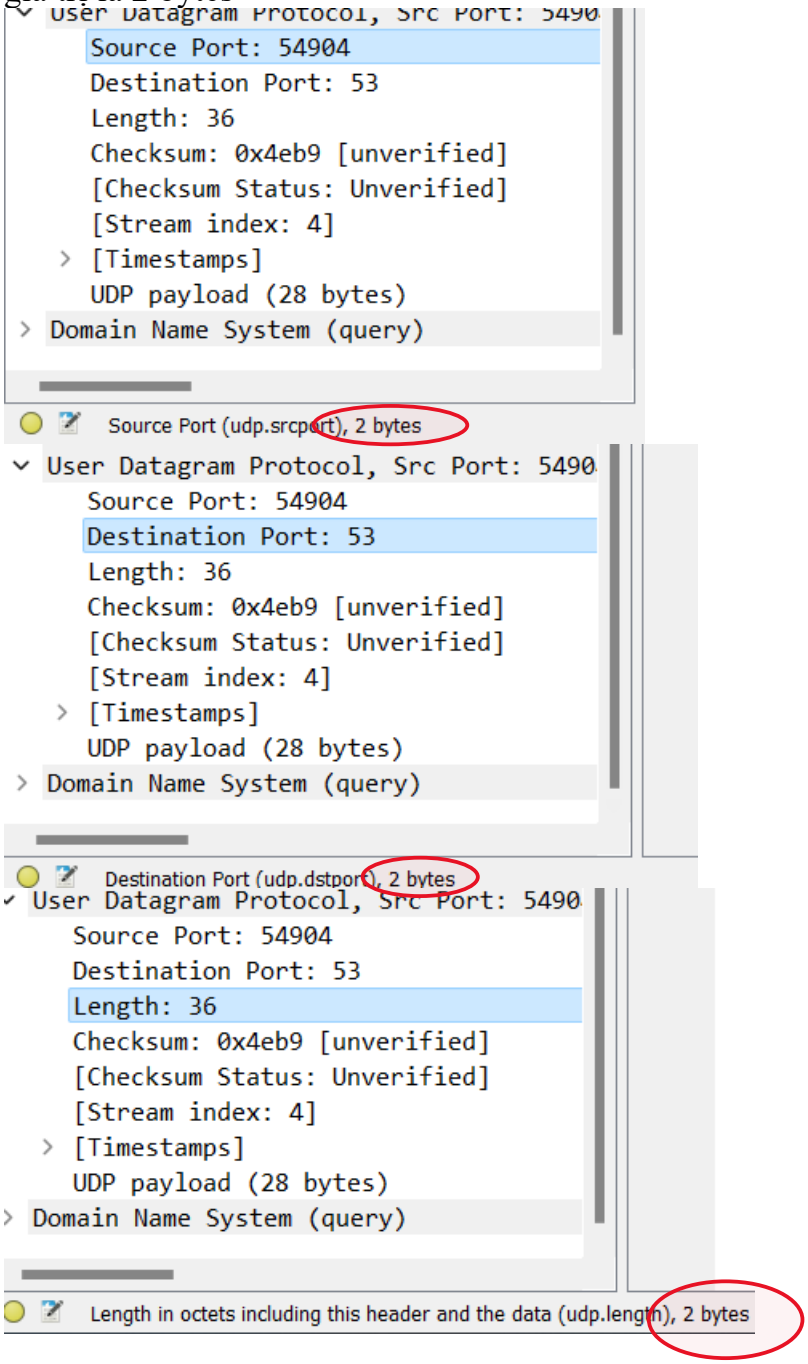
3. Chọn một gói tin DNS, xác định các trường (field) có trong UDP header và giải thích ý nghĩa của mỗi trường đó? Gợi ý: Xem tại phần User Datagram Protocol

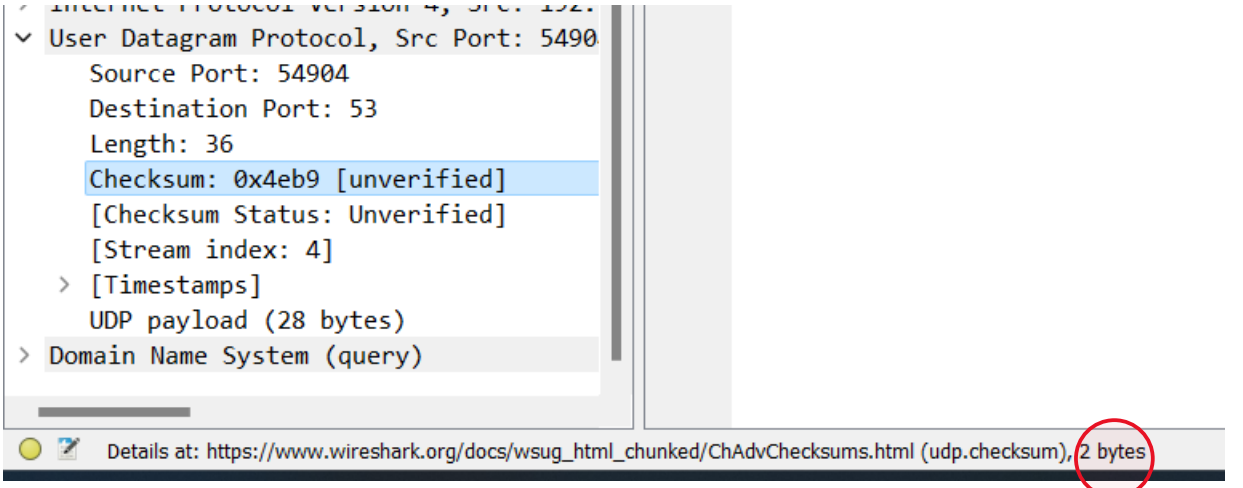


- Source port: Số hiệu cổng nơi đã gửi gói dữ liệu (datagram)
- Destination port: Số hiệu cổng nơi datagram được chuyển tới.
- Length: Độ dài tổng cộng kể cả phần header của gói UDP datagram.

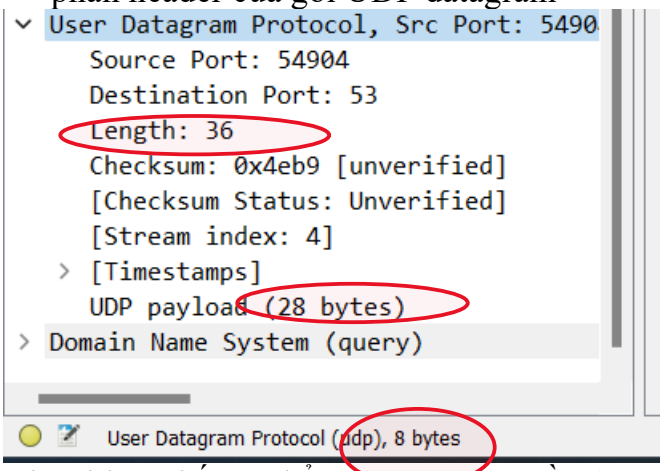
- Checksum: Trường checksum dùng cho việc kiểm tra lỗi của phần header và dữ liệu, nếu phát hiện lỗi thì UDP datagram sẽ bị loại bỏ mà không có thông báo trả về nơi gửi.

4. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?
   - Độ dài tính theo byte của mỗi trường trong UDP header qua wireshark đều có giá trị là 2 bytes

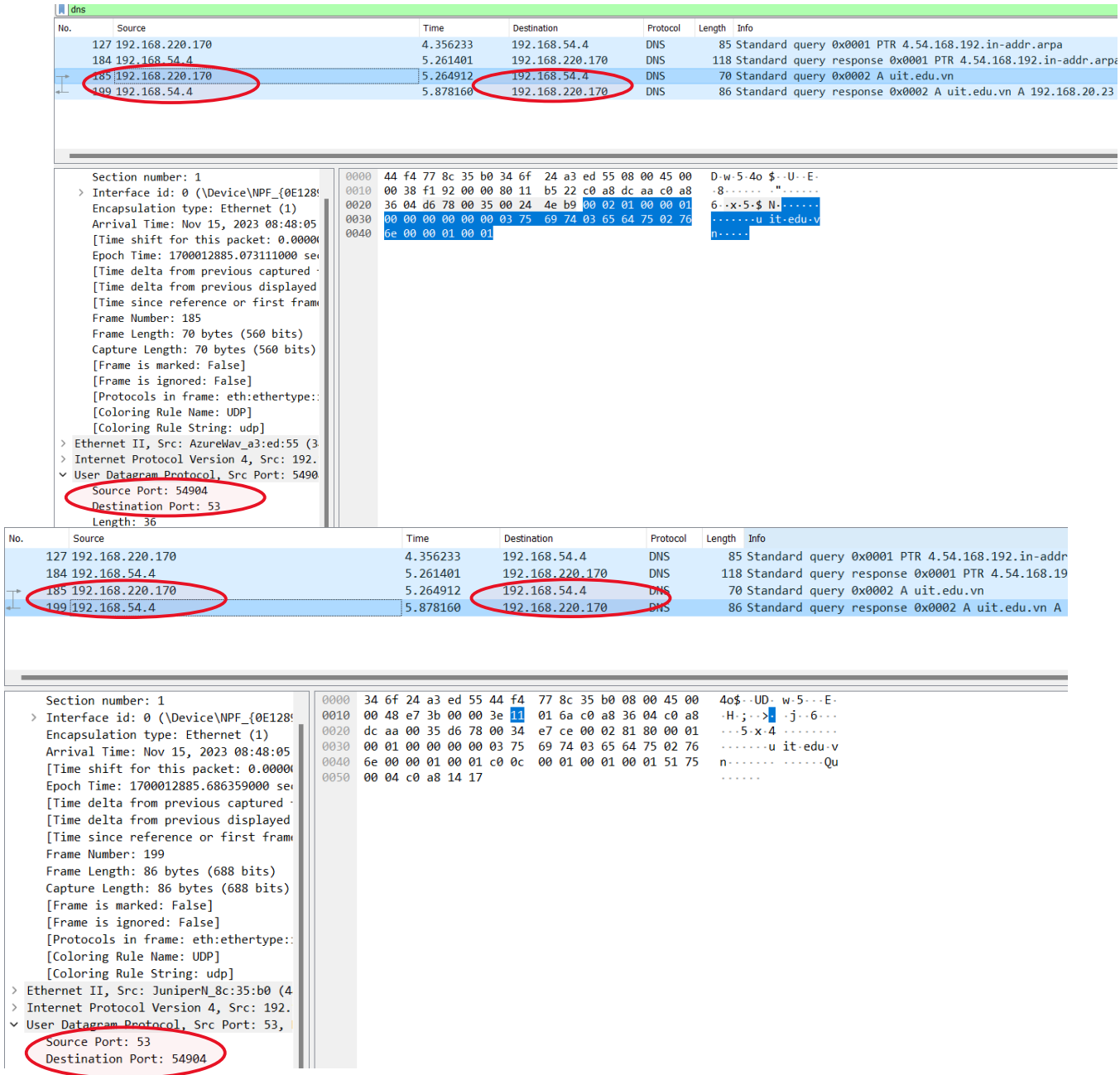




5. Giá trị của trường Length trong UDP header là độ dài của gì? Chứng minh nhận định này bằng thông tin hiển thị của Wireshark? Gợi ý: Quan sát kích thước payload (DNS Data) và kích thước UDP Header
   - Quan sát được UDP Header có kích thước là 8 bytes, và UDP payload có kích thước là 28 bytes là độ dài của gói datagram, có tổng bằng 36 bytes đúng bằng độ dài được hiển thị ở trường Length, điều này nghĩa là độ dài tổng cộng kể cả phần header của gói UDP datagram



6. Giá trị lớn nhất có thể có của port nguồn (Source port)? Gợi ý: Dựa vào kích thước (bytes) của trường Source port
   - Với trường kích thước là 2 bytes đã tìm ở câu 4, giá trị lớn nhất của port nguồn theo lí thuyết = 2^{16}-1 = 65535 bytes
7. Số bytes lớn nhất mà payload (phần chứa dữ liệu gốc, không tính UDP header và IP header) của UDP có thể chứa? Gợi ý: Dựa vào kích thước của trường Length trong UDP header và giá trị lớn nhất có thể thể hiện?
   - Theo kích thước của trường Length là 2 bytes đã tìm ở câu 4, kích thước tối đa theo lí thuyết là 2^{16}-1 = 65535 bytes
   - Bởi vì trường Length chứa cả độ dài header, nên số bytes lớn nhất mà payload có thể chứa phải trừ đi 8 bytes của header = 65535 – 8 = 65527 bytes
8. Quan sát 2 gói tin tìm được ở Câu 1 và 2, mô tả mối quan hệ giữa các địa chỉ IP và các port của 2 gói tin này. Gợi ý: Quan sát Source (IP, Port) và Destination (IP, Port) của 2 gói tin trên.

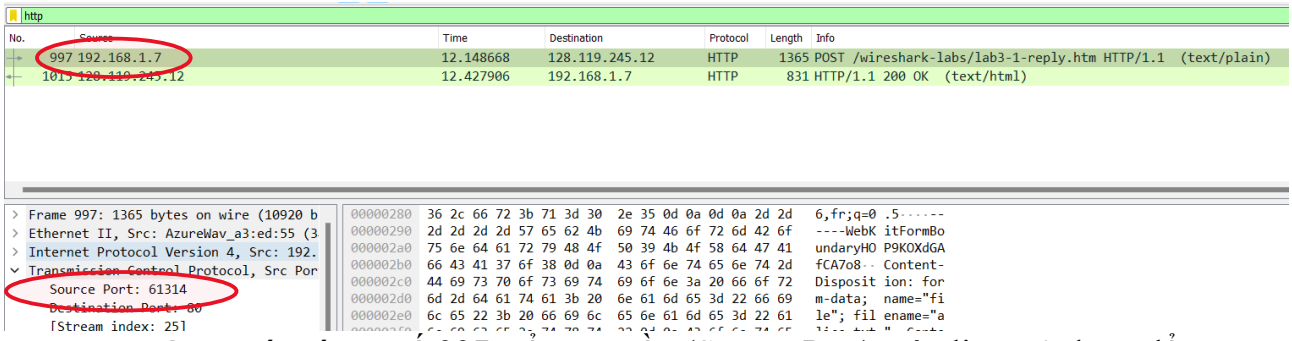


- Gói tin 185:
  + Source: IP 192.168.220.170, Port 54904
  + Destination: IP 192.168.54.4, Port 53
- Gói tin 199:
  + Source: IP 192.168.54.4, Port 53
  + Destination: IP 192.168.220.170, Port 54904
- Ta có thể quan sát được: gói tin 199 là gói tin phản hồi của gói tin 185, vì vậy nên phần source(IP, Port) của gói tin 185 là destination(IP, Port) của gói tin 199 và ngược lại

III. Upload file với Browser

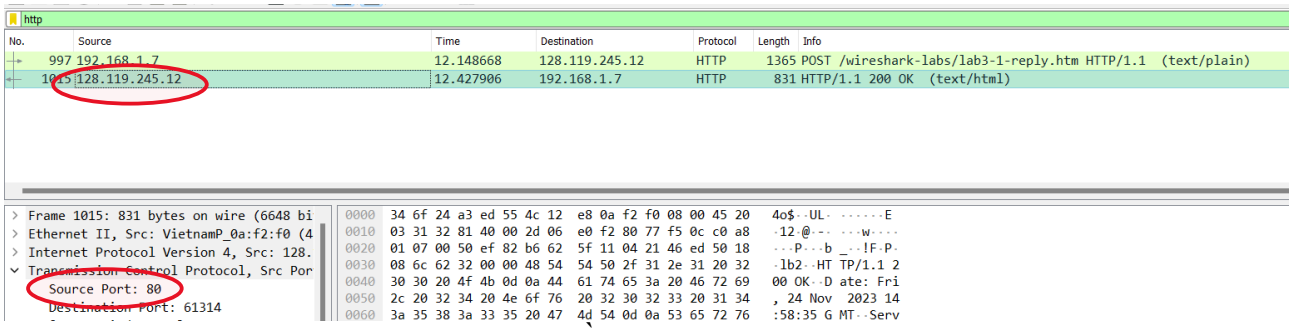
IV. Phân tích các gói tin TCP

9. Xác định Địa chỉ và cổng nguồn (Source Port) mà client sử dụng để chuyển tệp sang gaia.cs.umass.edu là gì? Gợi ý: Chọn một thông điệp HTTP từ Client gửi lên Server và khám phá các chi tiết của gói tin TCP được sử dụng để mang thông điệp HTTP này



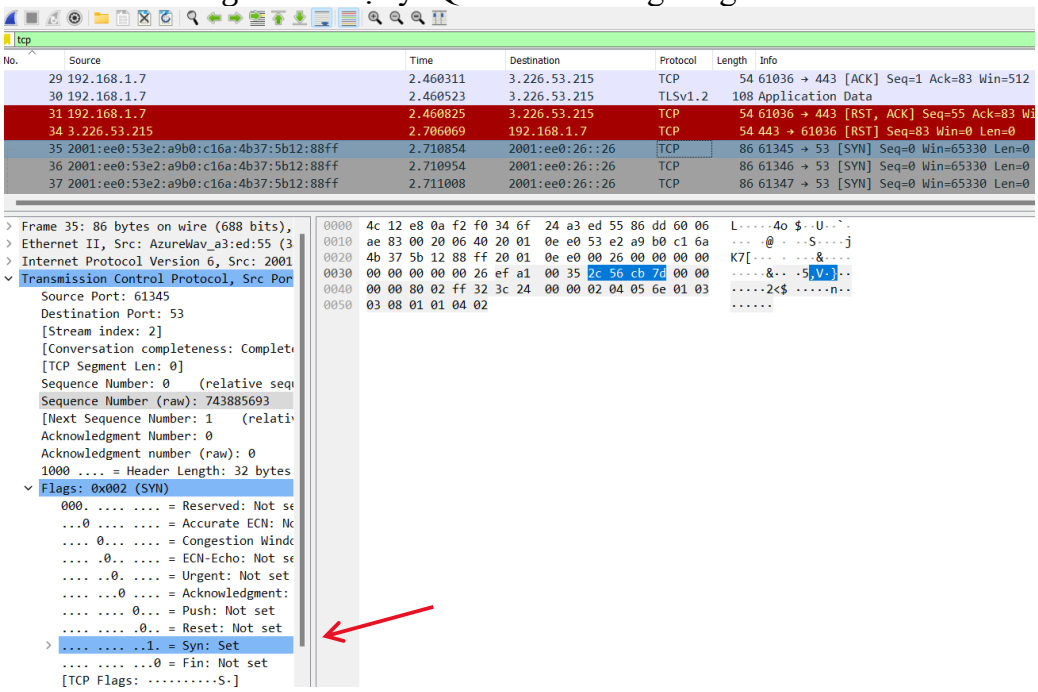
- Quan sát gói tin số 997, cổng nguồn (Source Port) mà client sử dụng để chuyển tệp sang gaia.cs.umass.edu là 61314, và địa chỉ IP của client là 192.168.1.7

10. Địa chỉ IP của gaia.cs.umass.edu là gì? Trên số cổng nào nó nhận các dữ liệu của tệp alice.txt



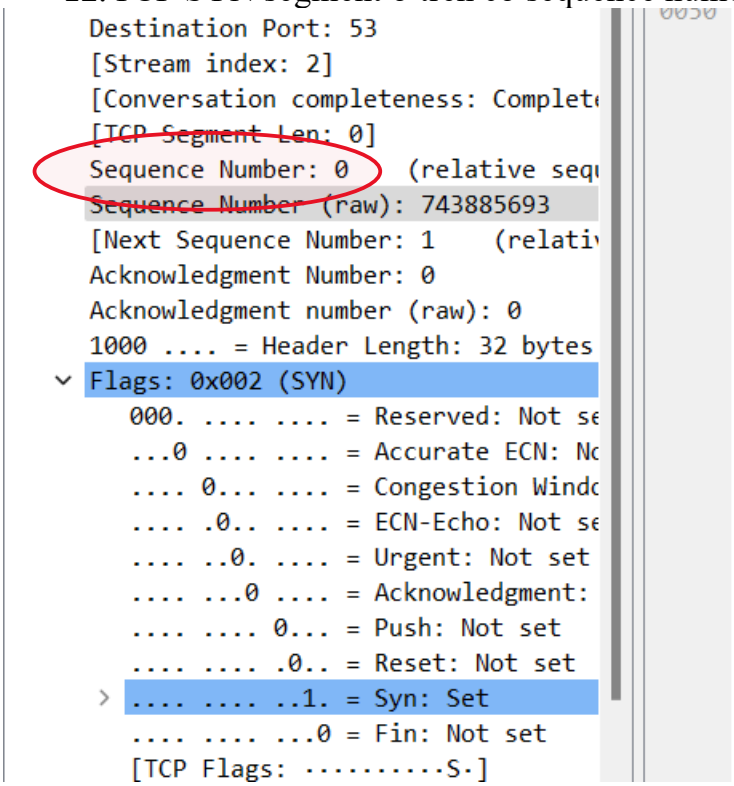
- Gói tin 1015 là gói tin phản hồi từ gaia.cs.umass.edu của gói tin 997, quan sát được địa chỉ IP của gaia.cs.umass.edu ở trường Source: 128.119.245.12, và số cổng là 80, quan sát được ở mục Source Port

11. Định vị TCP SYN segment (gói tin TCP có cờ SYN) 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



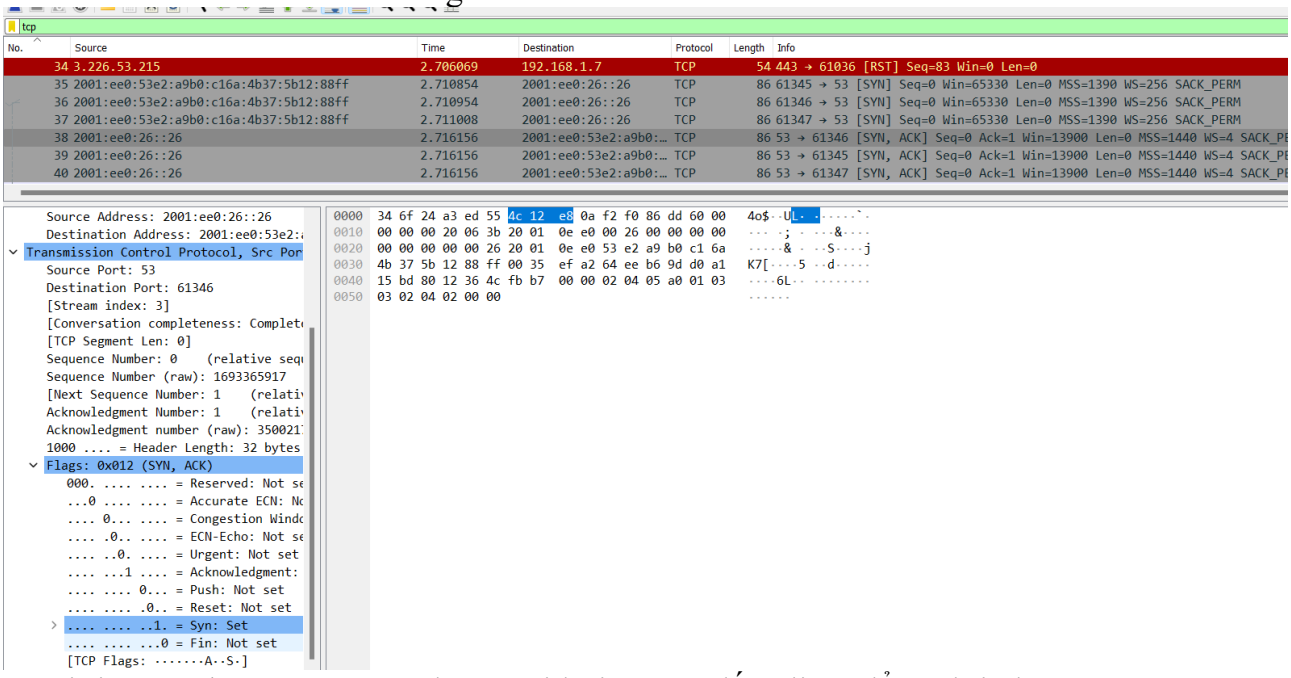
- Gói tin TCP có cờ SYN là gói tin thứ 35. Ta chọn gói tin vào phần tại trường Flags ta tìm dòng "Syn" nếu là giá trị "Set" và có cờ Syn là 1 vậy đây là TCP SYN segment.

12. TCP SYN segment ở trên có sequence number là bao nhiêu?



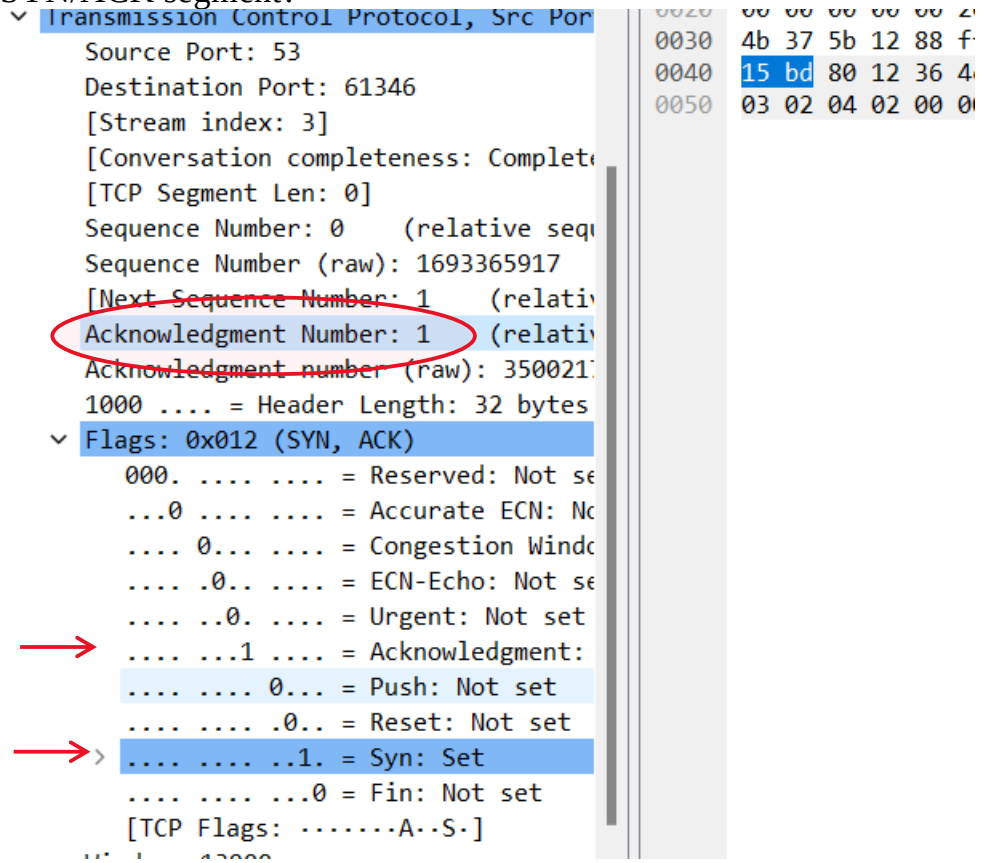
- TCP SYN segment ở trên có sequence number là : 0

13. Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment ở trên?



- Gói tin SYN/ACK segment được gửi bởi server đến client để trả lời cho SYN segment ở trên là gói tin 38, có sequence number = 0

14. 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?



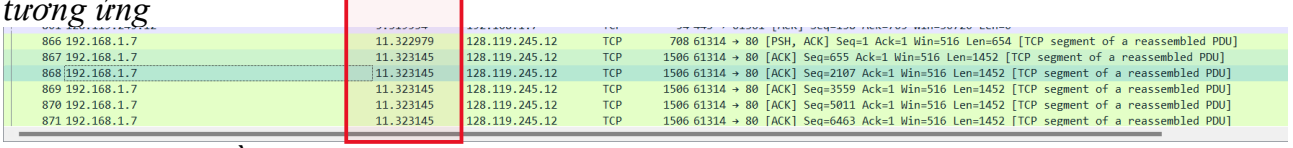
- Giá trị của Acknowledgement trong SYN/ACK segment là 1
- Sever xác định giá trị của Acknowledgement = X+1 với X là giá trị mà sequence number ở gói tin SYN mà client đã gửi trước đó.
- Thành phần cờ Acknowledgement và cờ Syn cho ta biết segment đó là SYN/ACK segment

15. Chỉ ra 6 segment đầu tiên mà Client gửi cho Server (dựa vào Số thứ tự gói – No) và liệt kê vào bảng dưới đây

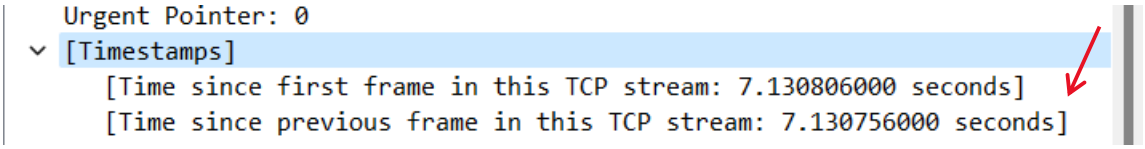
+ Tìm sequence number của 6 segments đầu tiên đó?

+ Xác định thời gian mà mỗi segment được gửi, thời gian ACK cho mỗi segment được nhận?

+ Tính RTT (Round Trip Time) cho 6 segments này. Biết RTT là khoảng thời gian tính từ lúc máy tính bắt đầu gửi segment cho đến khi nó nhận được ACK trả về tương ứng



- 6 segment đầu tiên mà Client gửi cho Server là các gói tin có No từ 866 -> 871, với sequence number lần lượt là 1, 655, 2107, 3559, 5011, 6463
- Có thể quan sát mốc thời gian mỗi segment được gửi ở mục time. Và dựa vào trường Timestamps để tìm ra RTT



- Từ đó, dễ dàng tính được mốc thời gian nhận ACK = mốc thời gian gửi segment + RTT

STT	Mốc thời gian gửi	Mốc thời gian nhận ACK	RTT (Round Trip Time)
866	11.322979	18.453735	7.130756
867	11.323145	11.323311	0.000166
868	11.323145	11.323145	0
869	11.323145	11.323145	0
870	11.323145	11.323145	0
871	11.323145	11.323145	0