3

Lab

**BÁO CÁO BÀI THỰC HÀNH SỐ 3**

**GIAO THỨC UDP & TCP**

**Môn học: NHẬP MÔN MẠNG MÁY TÍNH**

|  |  |
| --- | --- |
| **Sinh viên thực hiện** | Nguyễn Hải Thiện (23521481) |
| **Thời gian thực hiện** | 16/10/2024 – 26/10/2024 |
| **Số câu đã hoàn thành** | 14/14 |

**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.*

*Câu 1. Điền thông tin vào bảng sau*

***Trả lời:***

|  |  |
| --- | --- |
| *IP address* | *10.45.117.203* |
| *MAC address* | *88-D8-2E-27-43-18* |
| *Default gateway IP address* | *10.45.0.1* |
| *DNS server IP address* | *192.168.54.4*  *192.168.20.4* |

***Minh chứng:***

Mở Command Prompt, gõ lệnh ipconfig/all và nhấn Enter thì ta có thể xem các thông tin trên

A screenshot of a computer

Description automatically generated

* Xem IP Address ở dòng IPv4 Address
* Xem MAC Address ở dòng Physical Address
* Xem *Default gateway IP address ở dòng Default gateway*
* *DNS server IP address ở dòng DNS Severs*

*Câu 2. Tại danh sách các gói tin bắt được, định vị gói tin truy vấn domain google.com. Gợi ý: chứa "standard query" và "A www.google.com".*

***Trả lời:*** *là gói ở dòng 2305*

***Minh chứng:***

Vào bộ lọc Filter và gõ dns và sẽ thấy được gói tin truy vấn domain google.com nằm ở dòng 2305

*A screenshot of a computer

Description automatically generated*

*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*

***Trả lời:*** *là gói tin số 2340. Ip của domain goole.com là 217.160.0.201*

***Minh chứng:***

Xác định được gói tin 2340 là gói tin phản hồi của truy vấn trên vì ở cột Info có thông tin Standard query response A goole.com

Xem địa chỉ IP của domain google.com: vào phần Domain Name System của gói tin => Answer => xem addr

A screenshot of a computer

Description automatically generated

*Câu 4. 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*

***Trả lời:***

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

***Minh chứng:***

A screenshot of a computer

Description automatically generated

*Câu 5. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của*

*mỗi trường trong UDP header?*

***Trả lời:*** *Độ dài của mỗi trường trong UDP header là 2 bytes*

***Minh chứng:***

Xem ở dòng cuối cùng của Source Port và Destination Port đều có giá trị là 2 bytes

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

*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 trong UDP header là độ dài của toàn bộ gói tin UDP****, bao gồm cả phần* ***UDP header và phần dữ liệu*** *(payload).*

***Minh chứng:***

- Giá trị của trường Length trong UDP header có độ dài là 64 bits/8 bytes bao gồm cả header và datagram.

- Nhìn vào hình bên dưới, ta thấy trường Length bằng 35 bytes.

- Ở giá trị UDP payload của gói tin là: 27 bytes.

- Từ đó ta có thể nhận thấy rằng trường Length có độ dài : 35 – 27 = 8 bytes

A screenshot of a computer

Description automatically generated

*Câu 7. Quan sát 2 gói tin tìm được ở Câu 1 và 2, mô tả mối quan hệ giữa các địa*

*chỉ IP và port number của 2 gói tin này.*

***Trả lời:*** *Source Port và Destination của gói gửi có giá trị ngược với Source Port và Destination của gói phản hồi*

***Minh chứng:***

A screenshot of a computer

Description automatically generated

* Source Port và Destination của packet gửi:

A screen shot of a computer

Description automatically generated

* Source Port và Destination của gói phản hồi

A screen shot of a computer

Description automatically generated

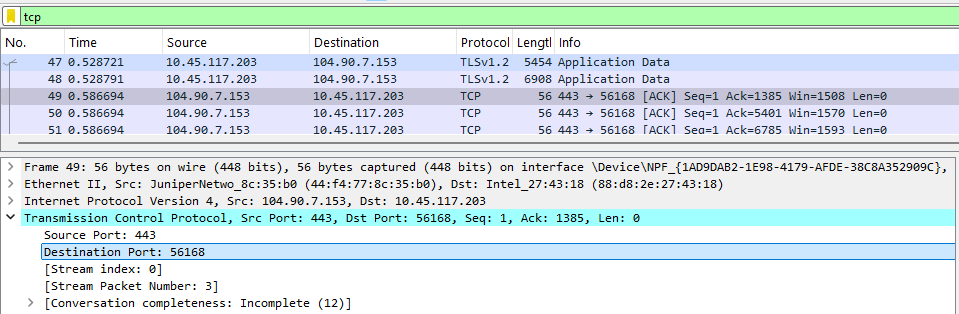
*Câu 8. Xác định IP và TCP port của client sử dụng để chuyển tệp sang gaia.cs.umass.edu là gì? Gợi ý: Chọn một thông điệp HTTP và khám phá các chi tiết của gói tin TCP được sử dụng để mang thông điệp HTTP này*

***Trả lời:*** *Địa chỉ IP của client: 10.45.117.203*

*Cổng TCP của client: 56168*

***Minh chứng:***

Để xác định địa chỉ IP của client, ta xem ở Destination của dòng 49. Để cổng TCP của client thì ta xem trong phần thông tin chi tiết, nằm ở dòng Destination Port



*Câu 9. Địa chỉ IP của gaia.cs.umass.edu là gì? Trên số cổng nào nó gửi và nhận*

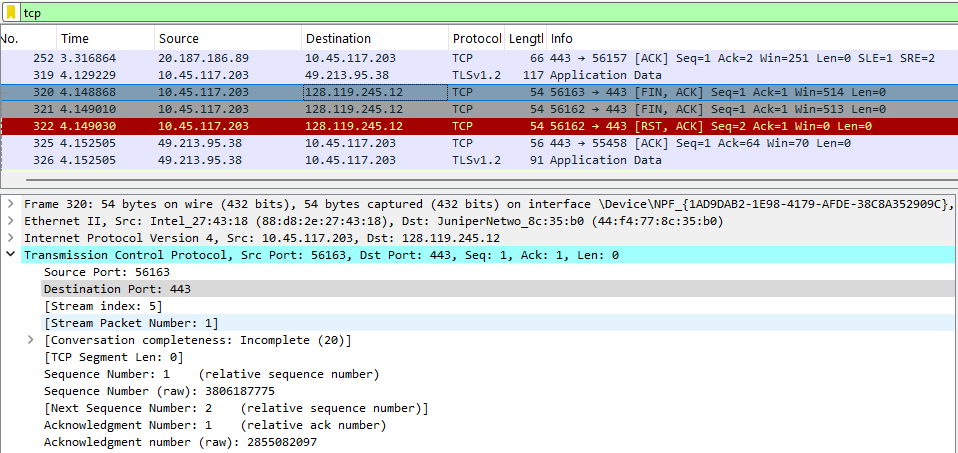
*các segment TCP cho kết nối này?*

***Trả lời:*** *Địa chỉ IP của gaia.cs.umass.edu: 128.119.245.12. Số cổng: 443*

***Minh chứng:***

Để xem địa chỉ IP của gaia.cs.umass.edu, ta có thể vào Terminal và gõ nslookup gaia.cs.umass.edu hoặc xem ở dòng 320, cột Destination.

Để xem số cổng mà nó gửi và nhận các segment TCP cho kết nối này thì ta xem trong phần thông tin chi tiết của gói 320, ở phần Destination Port là 443.



*Câu 10. TCP SYN segment (gói tin TCP có cờ SYN) sử dụng sequence number nào*

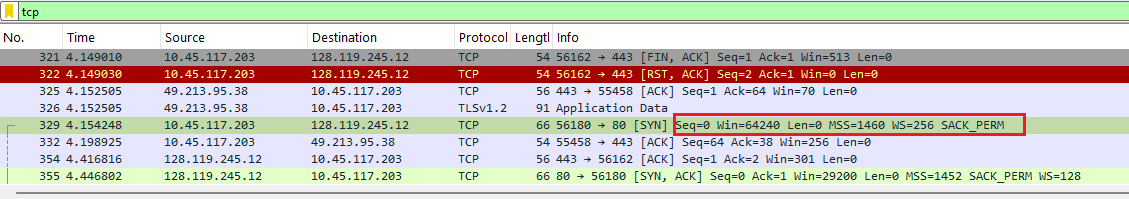
*để khởi tạo kết nối TCP giữa client và server? Thành phần nào trong segment*

*cho ta biết segment đó là TCP SYN segment? Gợi ý: Quan sát trường Flags.*

***Trả lời:*** *Sử dụng sequence number 0 để khởi tạo kết nói TCP giữa client và sever. Thành phần Flags trong segment cho ta biết segment đó là TCP SYN segment.*

***Minh chứng:***

Gói tin này sử dụng **Sequence Number** (số thứ tự) là **0** (trong phần Sequence Number (relative) được hiển thị là 0. Ở gói tin này, trường **Flags** cho thấy giá trị **0x002**. Điều này xác nhận rằng đây là một gói tin SYN, vì giá trị **0x002** trong trường Flags tương ứng với **SYN = 1**.



A screenshot of a computer program

Description automatically generated

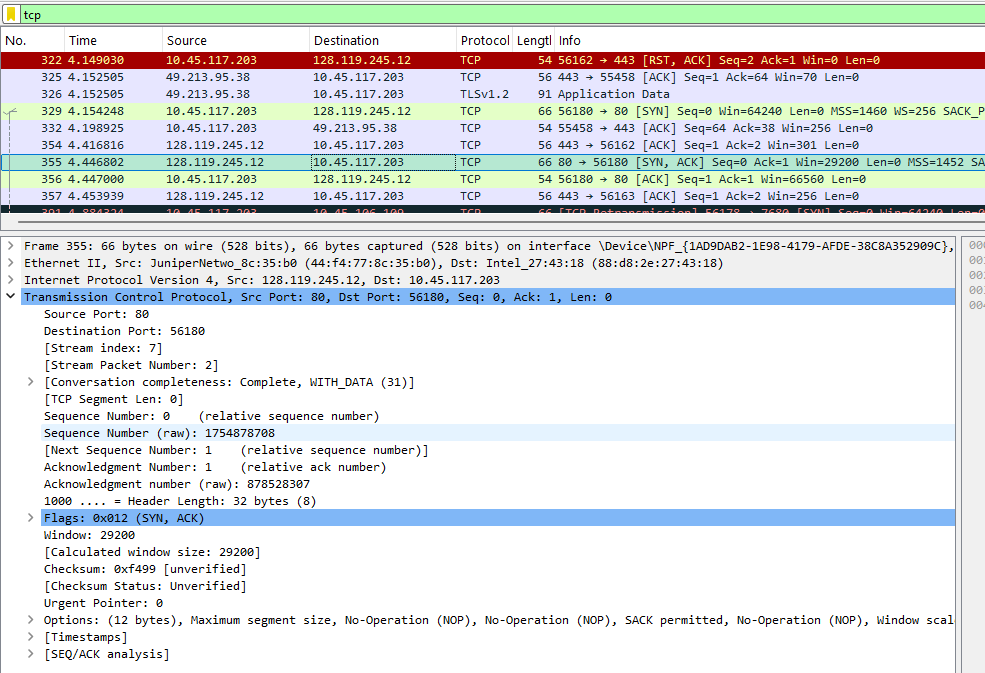
*Câu 11. Tìm sequence number của gói tin SYN/ACK segment được gửi bởi server*

*đến client để trả lời cho SYN segment?*

***Trả lời:*** *Sequence number =* ***1754878708***

***Minh chứng:***

Để xem Sequence number của gói tin SYN/ACK segment được gửi bởi sever đến client để trả lời cho SYN segment, ta xem phần thông tin chi tiết, ở dòng Sequence number (raw)



*Câu 12. Tìm gia trị cua Acknowledgement trong SYN/ACK segment? Làm sao*

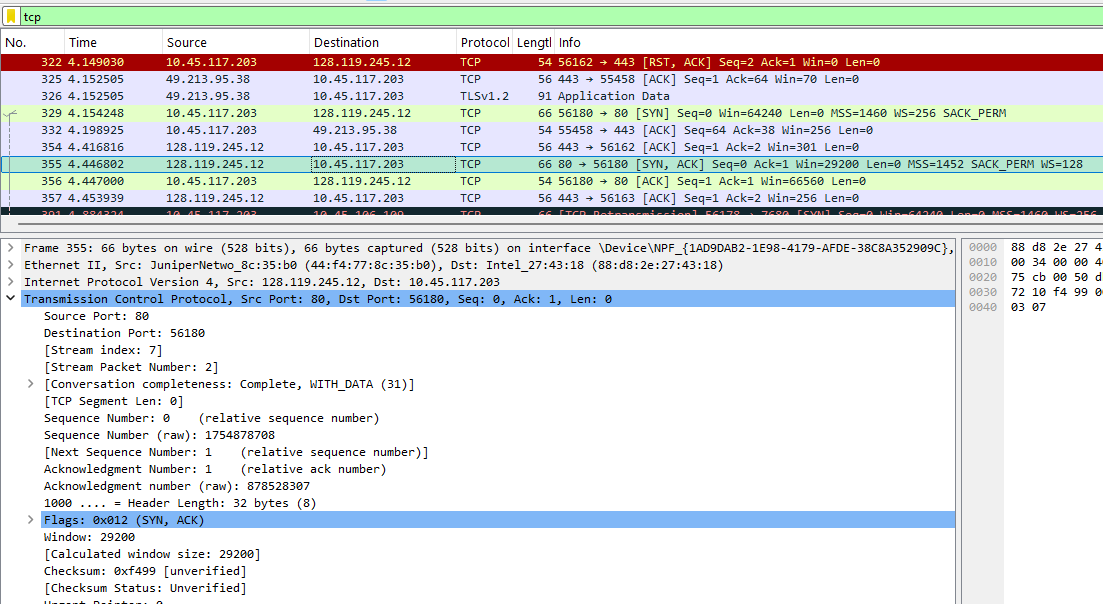
*server có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết*

*segment đó là SYN/ACK segment?*

***Trả lời:*** *Giá trị Acknowledgement (ACK) trong gói SYN/ACK (dòng 355) là 875823807****. Cờ SYN, ACK cho biết đây là gói SYN/ACK segment***

***Minh chứng:***

Để xem địa giá trị của Acknowledgement trong SYN/ACK segment, ta xem trong phần thông tin chi tiết ở phần Ackknowledment number (raw).

hf

* Các thành phần trong cờ SYN, ACK cho ta thấy hai dòng Acknowledgement và Syn đã được ‘Set’ với 1 bit ‘1’.

A blue and white rectangular box with text

Description automatically generated

*Câu 13. Tìm độ dài của từng segment trong bộ 6 segments đầu tiên trên? Tìm*

*lượng buffer còn trống nhỏ nhất mà bên nhận thông báo cho bên gửi trong*

*suốt truyền tin? Gợi ý: Buffer còn trống = giá trị Calculated window size (Win)*

*trong các gói ACK mà server báo về bên gửi. Kiểm tra trong tất cả các gói chứa*

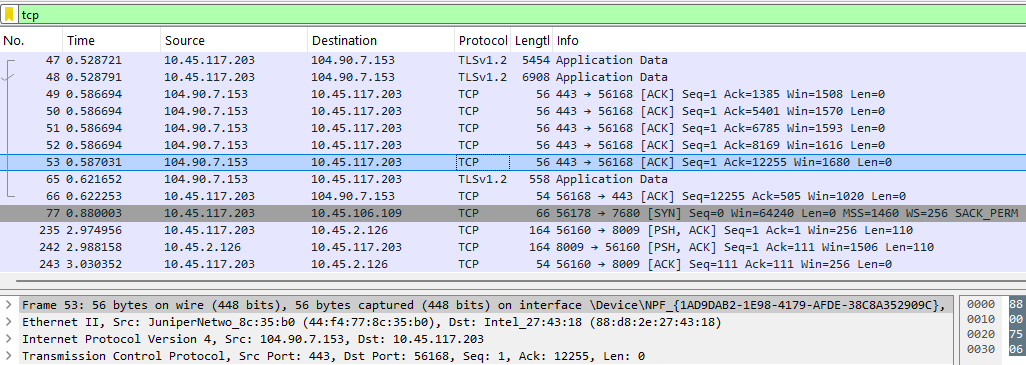
*ACK từ server trả về máy tính để xác định giá trị nhỏ nhất. Có thể chỉ lọc các*

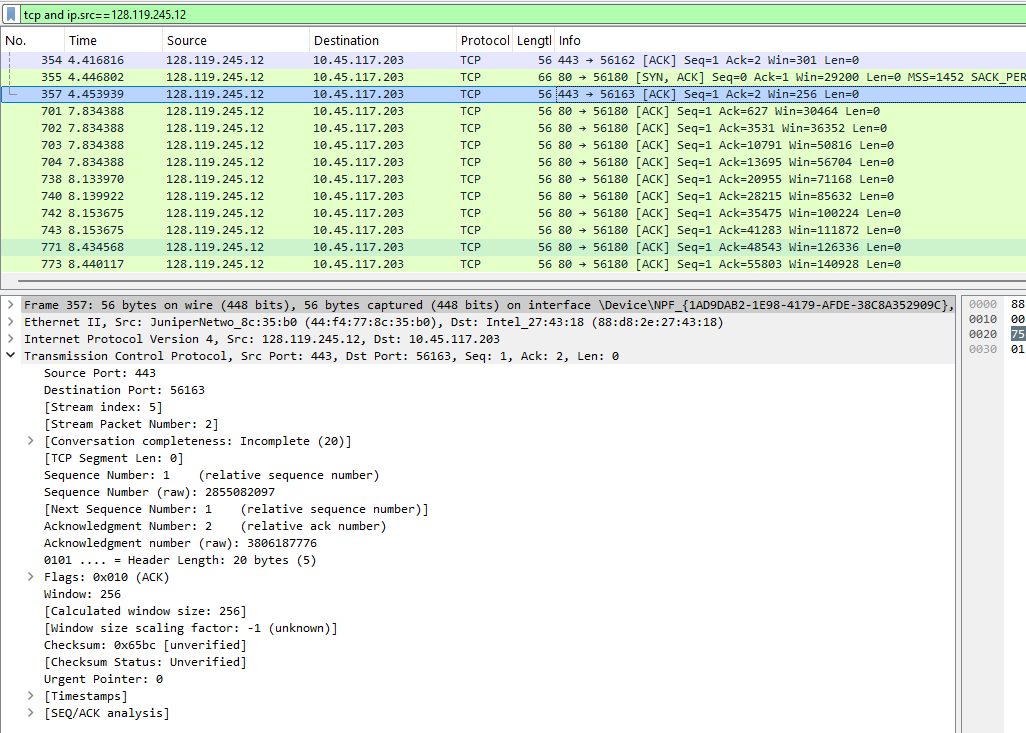
*gói từ server bằng cách thêm điều kiện filter "tcp and ip.src == IP của server"*

***Trả lời:*** *Độ dài của từng segment trong bộ 6 segment đầu tiên: 56, 56, 56, 56, 56, 56, 54. Lượng buffer nhỏ nhất: 256*

***Minh chứng:***

* Để xem độ dài của từng segment trong bộ 6 segment đâu tiên, ta xem ở cột Length của các gói tin 49, 50, 51, 52, 53, 66.
* Lượng buffer còn trống nhỏ nhất là 256, nằm ở gói tin 357





*Câu 14. Có segment nào được gửi lại hay không? Thông tin nào trong quá trình*

*truyền tin cho chúng ta biết điều đó?*

***Trả lời:*** *Có segment được gửi lại dựa vào biểu đồ. Ta thấy được từng thời điểm khác nhau mà segment được truyền lại do có 1 số packet bị trùng với sequence number (phần màu đỏ)*

***Minh chứng:***

A screenshot of a computer

Description automatically generated