Bài thực hành

Sử dụng Wireshark để quan sát quá trình bắt tay 3 bước của TCP

Mục tiêu

Sử dụng Wireshark để giám sát lưu lượng

Tạo lưu lượng TCP

Quan sát quá trình bắt tay 3 bước

Chuẩn bị

Sinh viên có phần mềm wireshark được cài đặt trên máy tính.

Sinh viên có kiến thức về TCP

Thực hiện

Bước 1: Bật Wireshark và bắt đầu bắt gói tin.

Bước 2: Truy cập vào website https://ntu.edu.vn/

Bước 3: Dừng bắt

Bước 4: Lọc lưu lượng bắt tay 3 bước sử dụng các cú pháp lọc:

- Lọc cổng ví dụ tcp.port==443
- Lọc cờ ví dụ tcp.flags.syn==1
- Nhiều điều kiện: kết hợp toán tử AND (&&) OR (||)

Bước 4: Phân tích lưu lượng bắt được

Câu 1. Trong gói tin bắt đầu quá trình bắt tay 3 bước:

Địa chỉ MAC nguồn, MAC đích là gì?

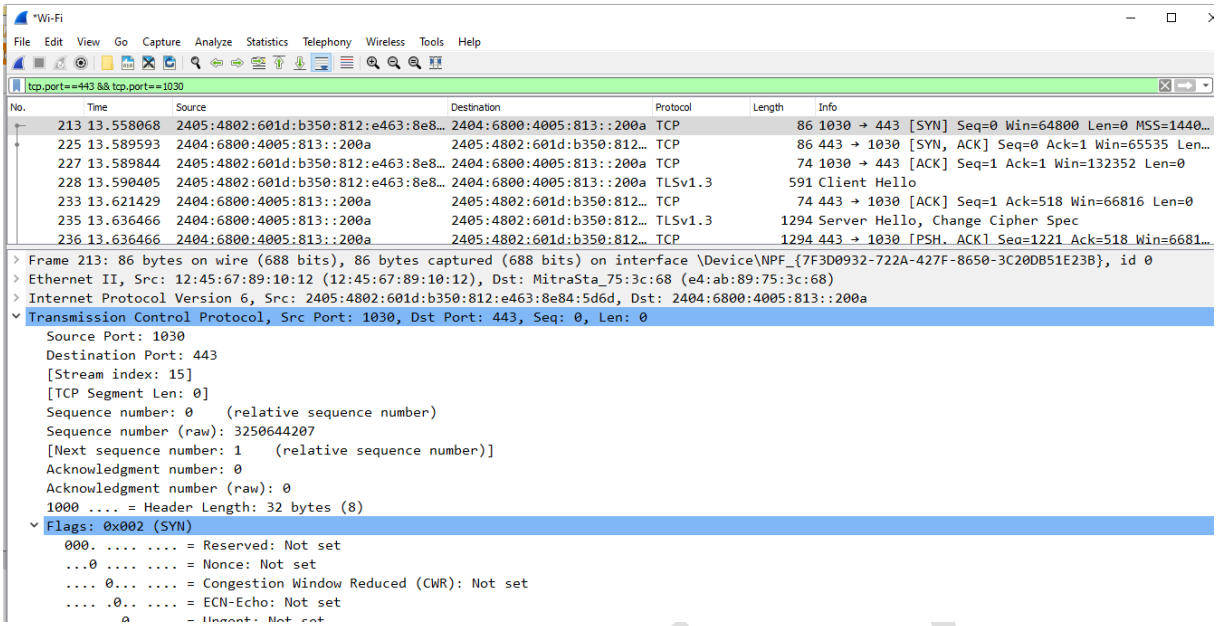
Địa chỉ IP nguồn, IP đích là gì?

Địa chỉ cổng nguồn, cổng đích là gì?

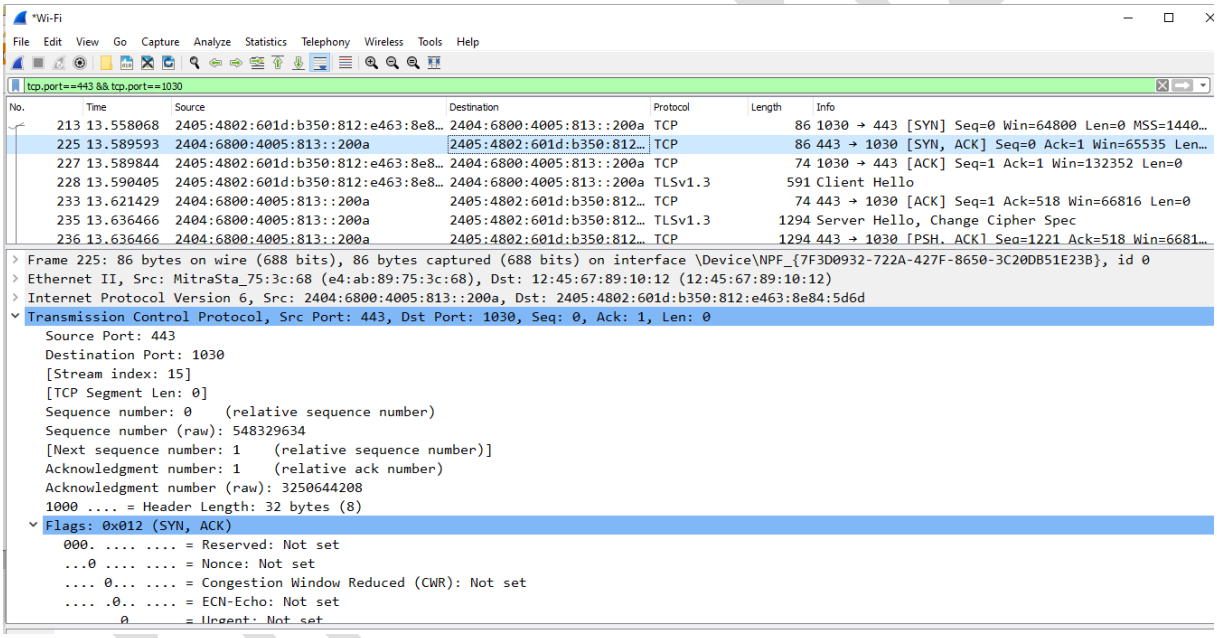
Cờ nào bật?

Giá trị Sequence number (raw) là gì? Ai thiết lập giá trị này? Nhận xét?

Giá trị acknowledgement number là gì? Ai thiết lập giá trị này? Nhận xét?



Câu 2: Trong gói tin trả về từ server tại bước thứ 2 hãy trả lời



Địa chỉ MAC nguồn, MAC đích là gì?

Địa chỉ IP nguồn, IP đích là gì?

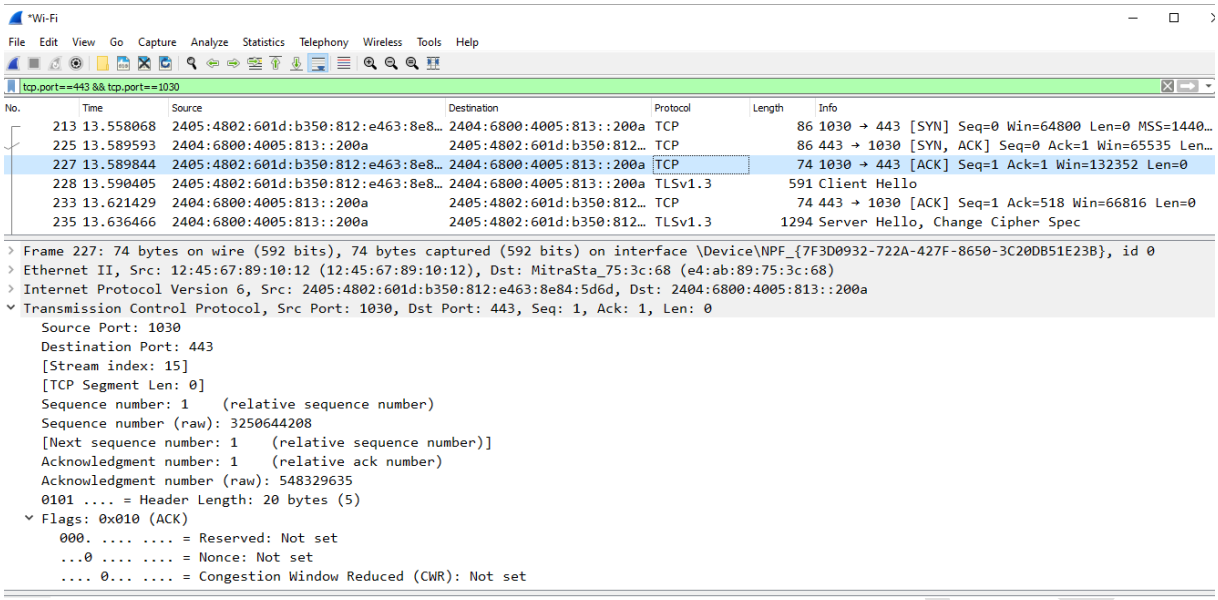
Địa chỉ cổng nguồn, cổng đích là gì?

Cờ nào bật?

Giá trị Sequence number (raw) là gì? Hãy nhận xét giá trị này?

Giá trị acknowledgement number là gì? Hãy nhận xét giá trị này?

Câu 3: Để hoàn thành bước cuối cùng của bắt tay 3 bước, client gửi gói tin đến server



Địa chỉ MAC nguồn, MAC đích là gì?

Địa chỉ IP nguồn, IP đích là gì?

Địa chỉ cổng nguồn, cổng đích là gì?

Cờ nào bật?

Giá trị Sequence number (raw) là gì? Hãy nhận xét giá trị này?

Giá trị acknowledgement number là gì? Hãy nhận xét giá trị này?

Câu 4: Hỏi RTT quá trình bắt tay ba bước hết bao nhiêu thời gian?

Câu 5: Chiều dài TCP header là bao nhiêu trong mỗi trường hợp gói tin?