

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?

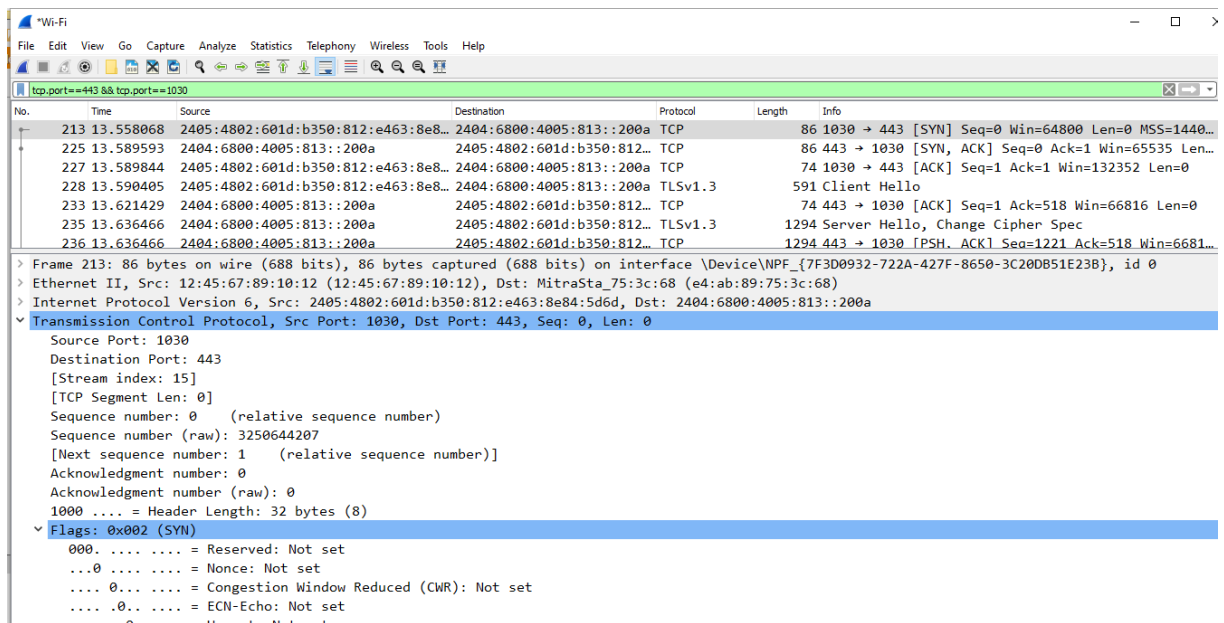
Địa chỉ IP nguồn, IP đích là gì?

Địa chỉ cổng nguồn, cổng đích là gì?

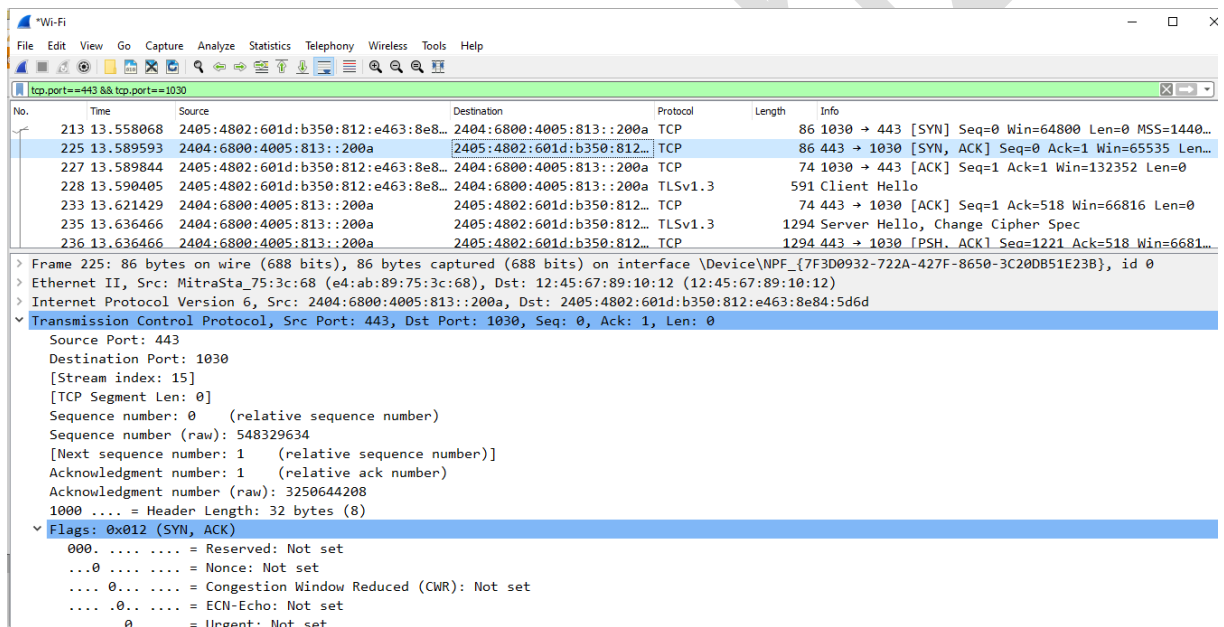
Cờ nào bật?

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

No.	Time	Source	Destination	Protocol	Length	Info
213	13.558068	2405:4802:601d:b350:812:e463:8e8...	2404:6800:4005:813::200a	TCP	86	1030 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440...
225	13.589593	2404:6800:4005:813::200a	2405:4802:601d:b350:812...	TCP	86	443 → 1030 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len...
227	13.589844	2405:4802:601d:b350:812:e463:8e8...	2404:6800:4005:813::200a	TCP	74	1030 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
228	13.590405	2405:4802:601d:b350:812:e463:8e8...	2404:6800:4005:813::200a	TLSv1.3	591	Client Hello
233	13.621429	2404:6800:4005:813::200a	2405:4802:601d:b350:812...	TCP	74	443 → 1030 [ACK] Seq=1 Ack=518 Win=66816 Len=0
235	13.636466	2404:6800:4005:813::200a	2405:4802:601d:b350:812...	TLSv1.3	1294	Server Hello, Change Cipher Spec

> Frame 227: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{7F3D0932-722A-427F-8650-3C20DB51E23B}, id 0

> Ethernet II, Src: 12:45:67:89:10:12 (12:45:67:89:10:12), Dst: MitraSta_75:3c:68 (e4:ab:89:75:3c:68)

> Internet Protocol Version 6, Src: 2405:4802:601d:b350:812:e463:8e84:5d6d, Dst: 2404:6800:4005:813::200a

▼ Transmission Control Protocol, Src Port: 1030, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

Source Port: 1030

Destination Port: 443

[Stream index: 15]

[TCP Segment Len: 0]

Sequence number: 1 (relative sequence number)

Sequence number (raw): 3250644208

[Next sequence number: 1 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Acknowledgment number (raw): 548329635

0101 = Header Length: 20 bytes (5)

▼ Flags: 0x010 (ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

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?