LAB04- PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC UDP VÀ TCP

1. MỤC ĐÍCH VÀ NỘI DUNG

1.1. Mục đích

Bài thí nghiệm này được thiết kế để trang bị cho sinh viên các kỹ năng sử dụng phần mềm Wireshark để bắt và lọc các gói tin UDP, TCP theo yêu cầu. Thông qua đó, sinh viên có thể quan sát và hiểu được các hoạt động quan trọng của hai giao thức này. Bên cạnh đó, thông qua việc vận dụng kiến thức lý thuyết, sinh viên có thể thực hiện các tính toán, giải thích kết quả đã quan sát được.

1.2. Yêu cầu đối với sinh viên

- Môi trường thực hành:
  - Sử dụng thành thạo các chức năng cơ bản của phần mềm Wireshark
  - Thực hiện thành thạo các thao tác trên hệ điều hành Windows, bao gồm các thao tác với thông số TCP/IP đã được hướng dẫn trong các bài thực hành trước.
- Kiến thức: Nắm vững kiến thức về tầng giao vận, các giao thức UDP và TCP.
- Viết báo cáo thực hành và nộp kết quả theo yêu cầu như sau:
  - Báo cáo (bản giấy) theo mẫu đã cung cấp
  - File lưu lượng **lab04.pcapng**(Kích thước không quá 1 MB) đặt trong thư mục có tên định dạng **TenSV_ MSSV_Lab04**.

1.3. Cơ sở lý thuyết

1.3.1. Giao thức UDP

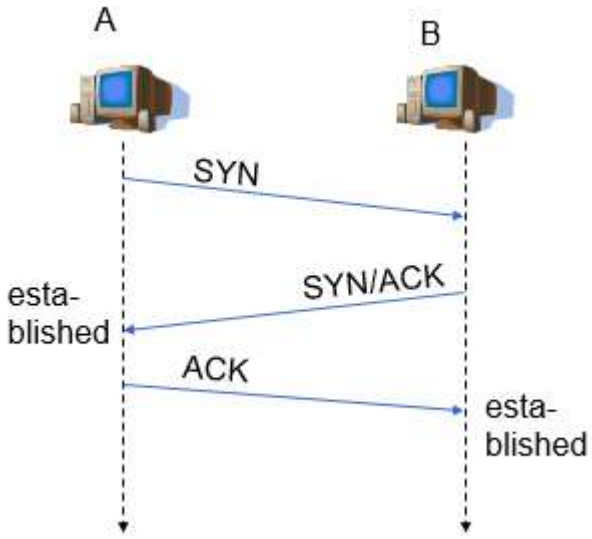
UDP (User Datagram Protocol) là một trong hai giao thức điều khiển truyền dữ liệu trên tầng giao vận trong mô hình TCP/IP. UDP hoạt động theo nguyên lý truyền thông hướng không liên kết(connectionless protocol). Theo đó, giao thức UDP nhận dữ liệu từ tiến trình của tầng ứng dụng, đóng gói vào các UDP datagram(gói tin UDP) và gửi ngay tới phía đích mà không cần thiết lập liên kết. Các gói tin UDP sẽ được phía đích nhận và xử lý một cách độc lập. Nếu gói tin không có lỗi, UDP sẽ chuyển lên cho tiến trình tương ứng của tầng ứng dụng; ngược lại nó sẽ hủy gói tin. Thêm vào đó, dù trong trường hợp nào đi chăng nữa, sẽ không có một gói tin báo nhận được gửi trả lại cho phía đích. Điều này dẫn đến một trong những đặc điểm quan trọng khác của UDP là truyền thông không tin cậy, nghĩa là quá trình điều khiển của UDP không đảm bảo truyền dữ liệu tới đích thành công. Nói một cách khác, phía nguồn chỉ truyền dữ liệu một lần và không cần biết dữ liệu có được truyền đi thành công

hay không. Chế độ truyền như vậy được gọi là chế độ best-effort. Bên cạnh đó, UDP sẽ thực hiện truyền liên tục dữ liệu với tốc độ cao nhất có thể. Điều này có thể gia tăng nguy cơ xảy ra tắc nghẽn trên đường truyền hoặc làm phía đích quá tải, không thể xử lý kịp thời dữ liệu nhận được.

1.3.2. Giao thức TCP

TCP (Transmission Control Protocol) là giao thức có cách hoạt động rất phức tạp so với UDP. Trước hết, TCP tuân theo nguyên lý của truyền thông hướng liên kết (connection-oriented), trong đó quá trình truyền gồm 3 giai đoạn: thiết lập liên kết, truyền dữ liệu và đóng liên kết. Để phục vụ việc quản lý và thông báo trạng thái liên kết giữa các bên, giao thức TCP thiết kế gói tin với các cờ điều khiển trong phần tiêu đề.

Ý nghĩa của quá trình thiết lập liên kết trong giao thức TCP là phía nguồn chỉ gửi dữ liệu khi nào phía đích đã sẵn sàng. Quá trình này thực hiện theo giao thức bắt tay 3 bước(three-handshake protocol):



- Bước 1: Phía yêu cầu(A) gửi một gói tin TCP không có phần thân(payload), có cờ SYN trong tiêu đề gói tin được bật.
- Bước 2: Nếu phía đáp ứng(B) sẵn sàng thiết lập liên kết, nó gửi gói tin với hai cờ SYN và ACK được bật. Gói tin này cũng không có phần thân.
- Bước 3: Phía yêu cầu gửi gói tin với cờ ACK được bật để xác nhận liên kết đã được thiết lập. Gói tin này có thể có phần payload.

Trên liên kết đã được thiết lập, dữ liệu của tiến trình tầng ứng dụng chuyển xuống được TCP đóng gói thành các TCP segment (gói tin TCP) và truyền đi bằng kỹ thuật truyền dòng (byte stream). Trong kỹ thuật này, phía nguồn sẽ đánh số thứ tự(Sequence Number) cho các gói tin gửi đi, còn phía nhận nếu cần sẽ sắp xếp các gói tin này theo đúng thứ tự và hợp lại thành một thông điệp gửi lên cho tiến trình tầng ứng dụng. Với cách truyền như vậy, rất có thể một thông điệp này sẽ dính theo dữ liệu của các thông điệp khác, tức là biên của các thông điệp là không rõ ràng. Các tiến trình của tầng ứng dụng phải sử dụng một cách thức nào đó để phân tách các thông điệp.

Bên cạnh đó, TCP là một giao thức truyền thông tin cậy. Phía gửi luôn biết rằng dữ liệu mà nó truyền đi có được truyền thành công hay không. Bởi vì giao thức TCP quy định rằng phía đích phải gửi gói tin báo nhận cho phía nguồn với cờ ACK được bật. Trong tiêu đề của gói tin này, giá trị ACK Number cho biết số thứ tự của dữ liệu mà phía đích cần nhận. Nếu phía nguồn xác định có lỗi xảy ra, dữ liệu trước đó sẽ được gửi lại; ngược lại dữ liệu tiếp theo được gửi đi. Sau khi hoàn thành việc truyền dữ liệu, các bên thực hiện các thao tác thỏa thuận đóng liên kết một cách tin cậy bằng cách gửi gói tin có cờ FIN được bật và để chắc chắn tất cả dữ liệu đã được nhận thành công.

Cuối cùng, để quá trình truyền không làm tắc ngẽn đường truyền và quá tải cho phía đích, giao thức TCP sử dụng cơ chế điều khiển tắc nghẽn và điều khiển luồng để giới hạn kích thước dữ liệu được gửi đi trong một lần truyền.

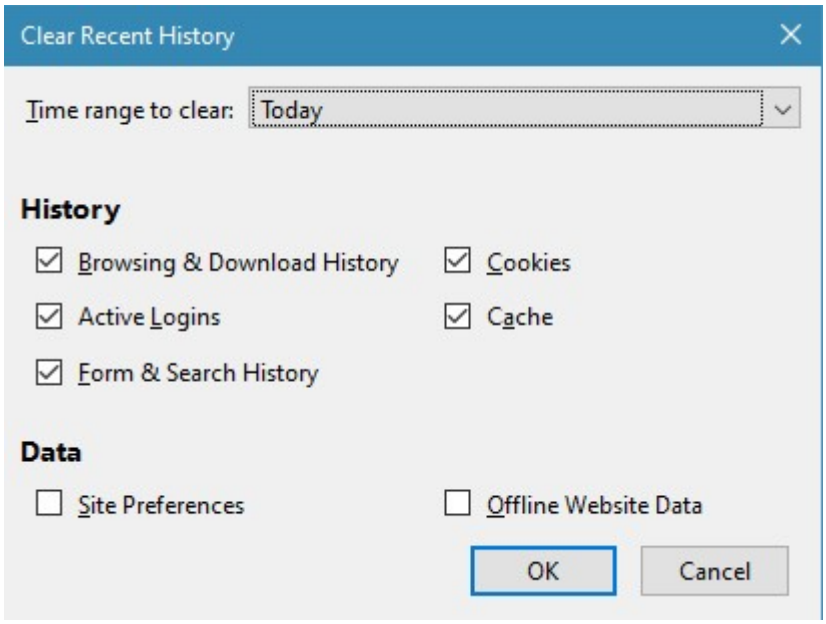
2. NỘI DUNG THỰC HÀNH

2.1. Xác định thông số của máy trạm

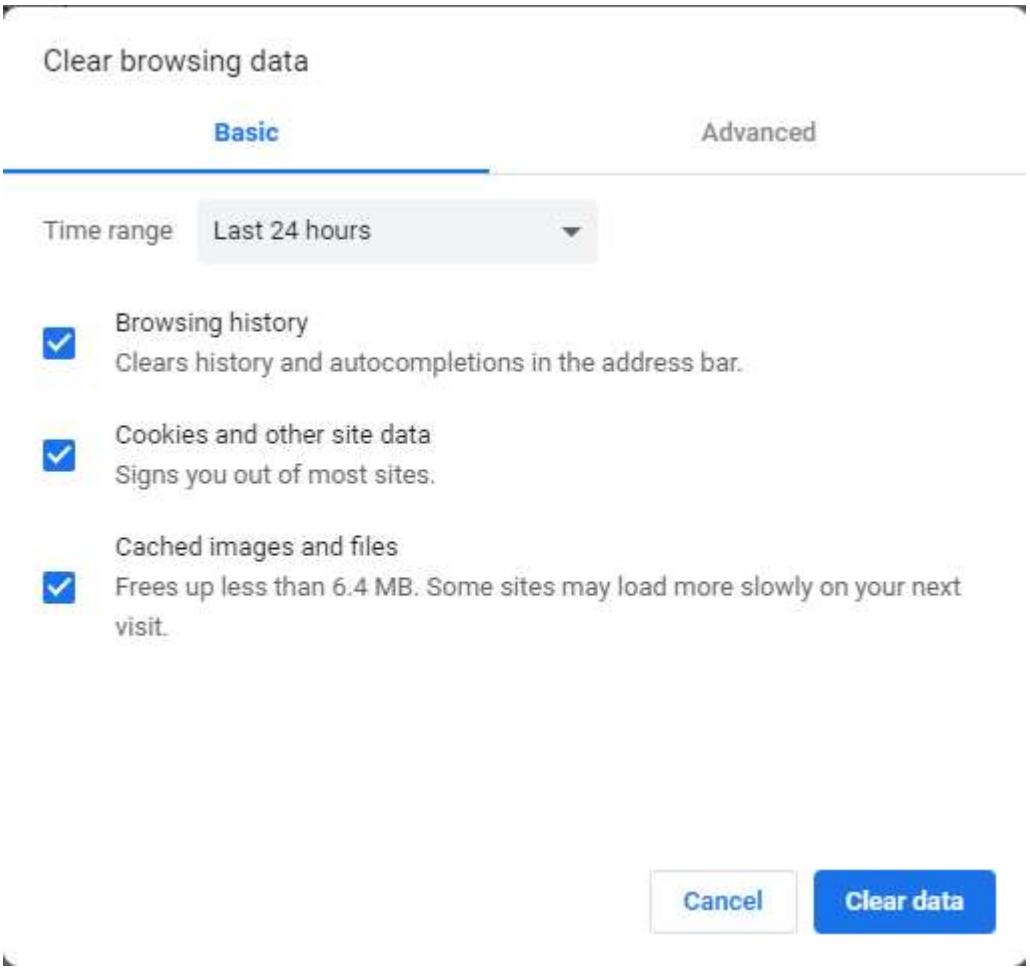
Sinh viên xác định địa chỉ IP trên máy tính ở phòng thực hành và ghi vào báo cáo. Để có được thông tin này, sinh viên xem lại bài thực hành số 2 và 3.

2.2. Thu thập lưu lượng mạng

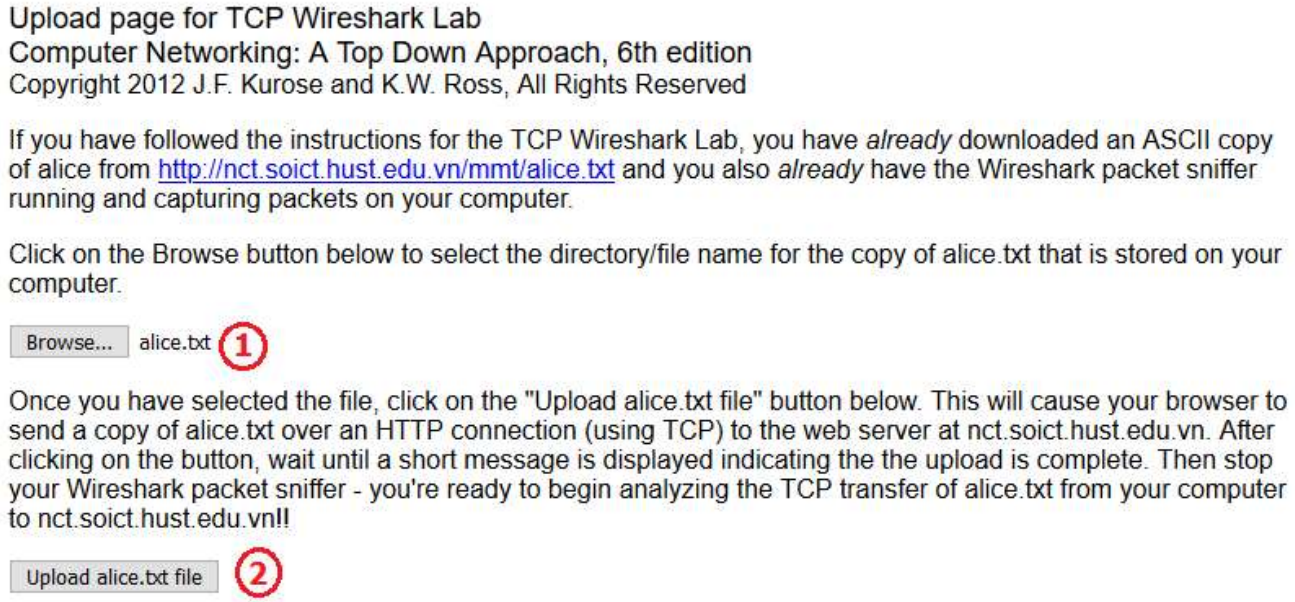
- **Bước 1:** Tắt các chương trình của người dùng có trao đổi dữ liệu trên mạng trừ trình duyệt Web để có thể quan sát quá trình truyền dữ liệu dưới đây một cách tốt nhất.
- **Bước 2:** Download file sau: http://nct.soict.hust.edu.vn/mmt/alice.txt
- **Bước 3:** Xóa bộ đệm của trình duyệt
  - Mozilla Firefox: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn các mục như dưới đây và nhấn OK.



- Google Chrome: Nhấn tổ hợp phím Ctrl + Shift + Del. Chọn the past day. Chọn Cached images and files. Nhấp nút Clear data.



- **Bước 4:** Trên cửa sổ Command Prompt, thực hiện lệnh ipconfig /flushdns
- **Bước 5:** Khởi động phần mềm Wireshark và chọn bắt gói tin trên card mạng phù hợp
- **Bước 6:** Quay trở lại cửa sổ trình duyệt, upload file alice.txt đã download ở bước số 2



- **Bước 8:** Sau khi thông báo hiển thị upload file thành công xuất hiện, đợi thêm khoảng 30 giây và dừng bắt gói tin trên Wireshark. Hình ảnh lưu lượng bắt được trên Wireshark có một phần tương tự như hình ảnh sau:

2	0.839954	192.168.1.176	8.8.8.8	DNS	81 Standard query 0x1c59 A nct.soict.hust.edu.vn
3	0.906865	8.8.8.8	192.168.1.176	DNS	97 Standard query response 0x1c59 A nct.soict.hust.edu.vn A 202.191.56.66
4	0.908215	192.168.1.176	202.191.56.66	TCP	66 5729 → 80 [SYN] Seq=2221575575 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5	0.908536	192.168.1.176	8.8.8.8	DNS	81 Standard query 0x6d03 A nct.soict.hust.edu.vn
6	0.910222	202.191.56.66	192.168.1.176	TCP	66 80 → 5729 [SYN, ACK] Seq=943466327 Ack=2221575576 Win=29200 Len=0 MSS=1460
7	0.910378	192.168.1.176	202.191.56.66	TCP	54 5729 → 80 [ACK] Seq=2221575576 Ack=943466328 Win=131328 Len=0
8	0.913761	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221575576 Ack=943466328 Win=131328 Len=1460
9	0.913761	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221577036 Ack=943466328 Win=131328 Len=1460
10	0.913764	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221578496 Ack=943466328 Win=131328 Len=1460
11	0.913764	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221579956 Ack=943466328 Win=131328 Len=1460
12	0.913764	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221581416 Ack=943466328 Win=131328 Len=1460
13	0.913765	192.168.1.176	202.191.56.66	TCP	946 5729 → 80 [PSH, ACK] Seq=2221582876 Ack=943466328 Win=131328 Len=892
14	0.913936	192.168.1.176	202.191.56.66	TCP	1514 5729 → 80 [ACK] Seq=2221583768 Ack=943466328 Win=131328 Len=1460

Lưu ý:

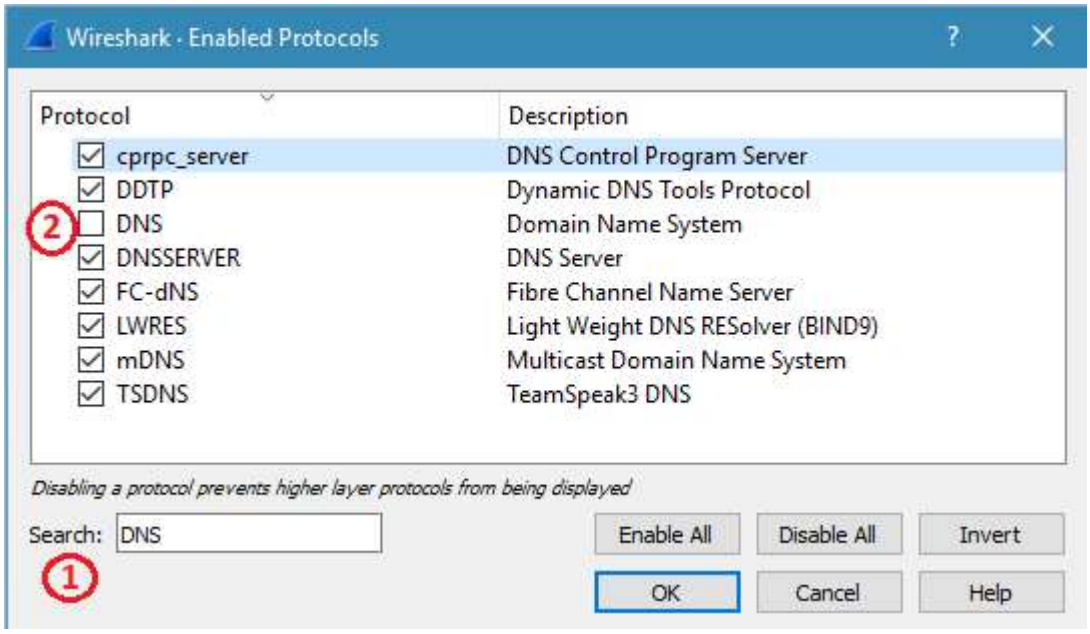
- *Nếu file lưu lượng trên máy sinh viên không có các gói tin có Protocol là DNS thì thực hiện lại từ bước 3.*
- *Các gói tin bắt được trên máy sinh viên có thể sẽ có một số thông số khác với hình ảnh minh họa. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành*

- **Bước 9:** Lưu file lưu lượng có tên là **lab04.pcapng** và nộp cùng báo cáo thực hành

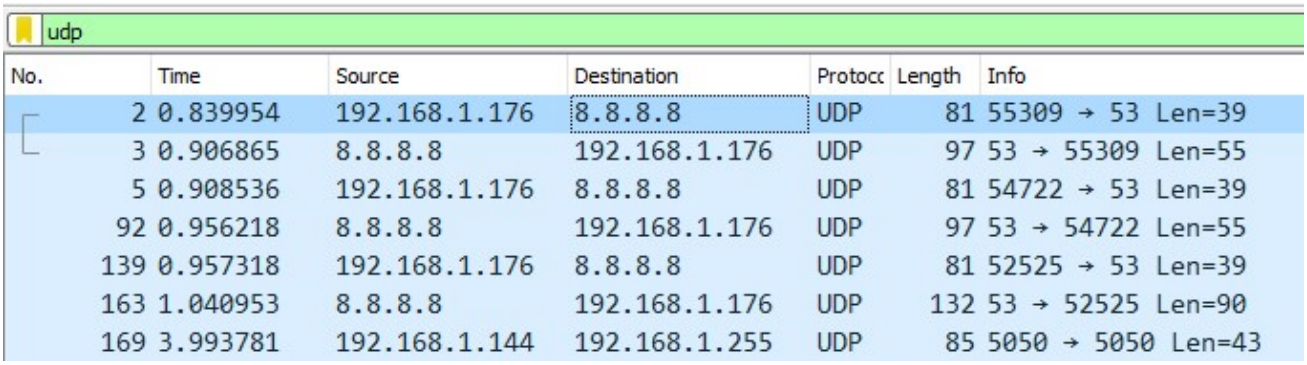
2.3. Quan sát các gói tin UDP

Sử dụng file lưu lượng ở mục 3.2 để quan sát và trả lời các câu hỏi.

- **Bước 1**: Trên menu của Wireshark, chọn **Analyze → Enabled Protocols**. Điền DNS vào ô **Search** và bỏ chọn mục DNS trong danh sách Protocol như hình dưới đây sau. Nhấn OK để đóng cửa sổ.



- **Bước 2:** Điền giá trị **udp** vào mục Filter của Wireshark để lọc ra các gói tin UDP đã bắt được tương tự như hình minh họa dưới đây.



- **Bước 3**: Chọn một gói tin UDP được gửi đi từ máy của sinh viên và trả lời câu hỏi 1.

Câu hỏi 1(1 điểm): Xác định các thông số sau của gói tin.STT gói

tin(No.):……..

Địa chỉ IP nguồn:…… Địa chỉ IP đích:……

Số hiệu cổng nguồn:…….. Số hiệu cổng đích:……

Gói tin này được đóng gói vào gói tin của giao thức tầng mạng nào?

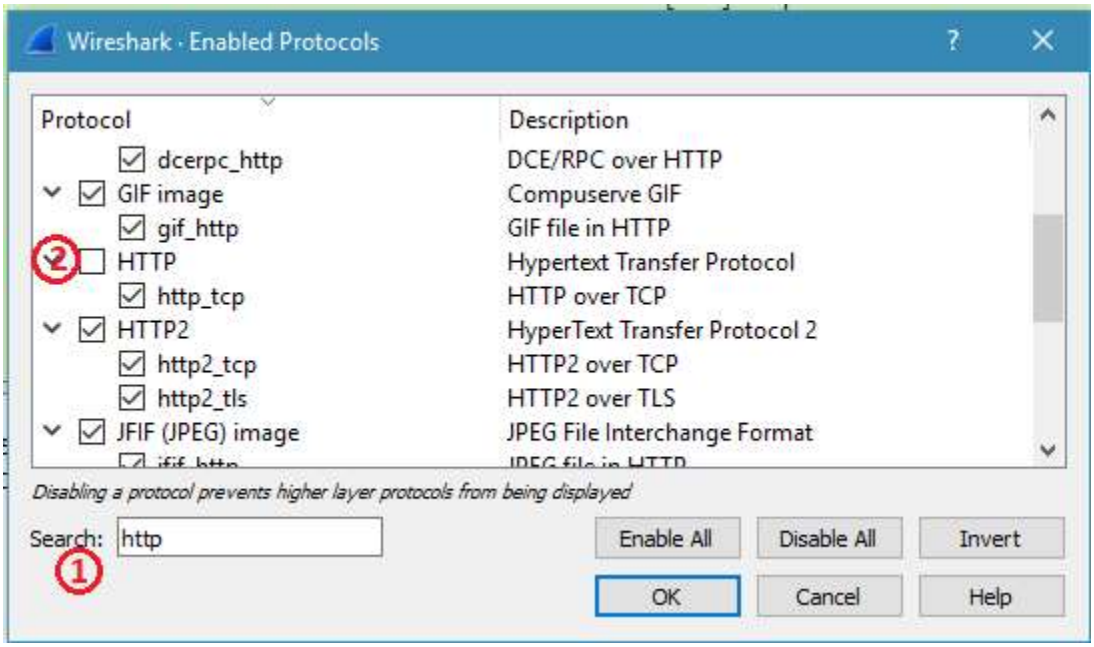
- **Bước 4:** Tìm gói tin mà máy đích trả lời cho gói tin ở bước 3 và trả lời câu hỏi 2.

Câu hỏi 2(1 điểm): STT gói tin:…..Tại sao xác định được đây là gói tin trả lời cho gói tin ở bước 3? Máy đích có thể biết được gói tin này đã được truyền thành công hay không? Tại sao?

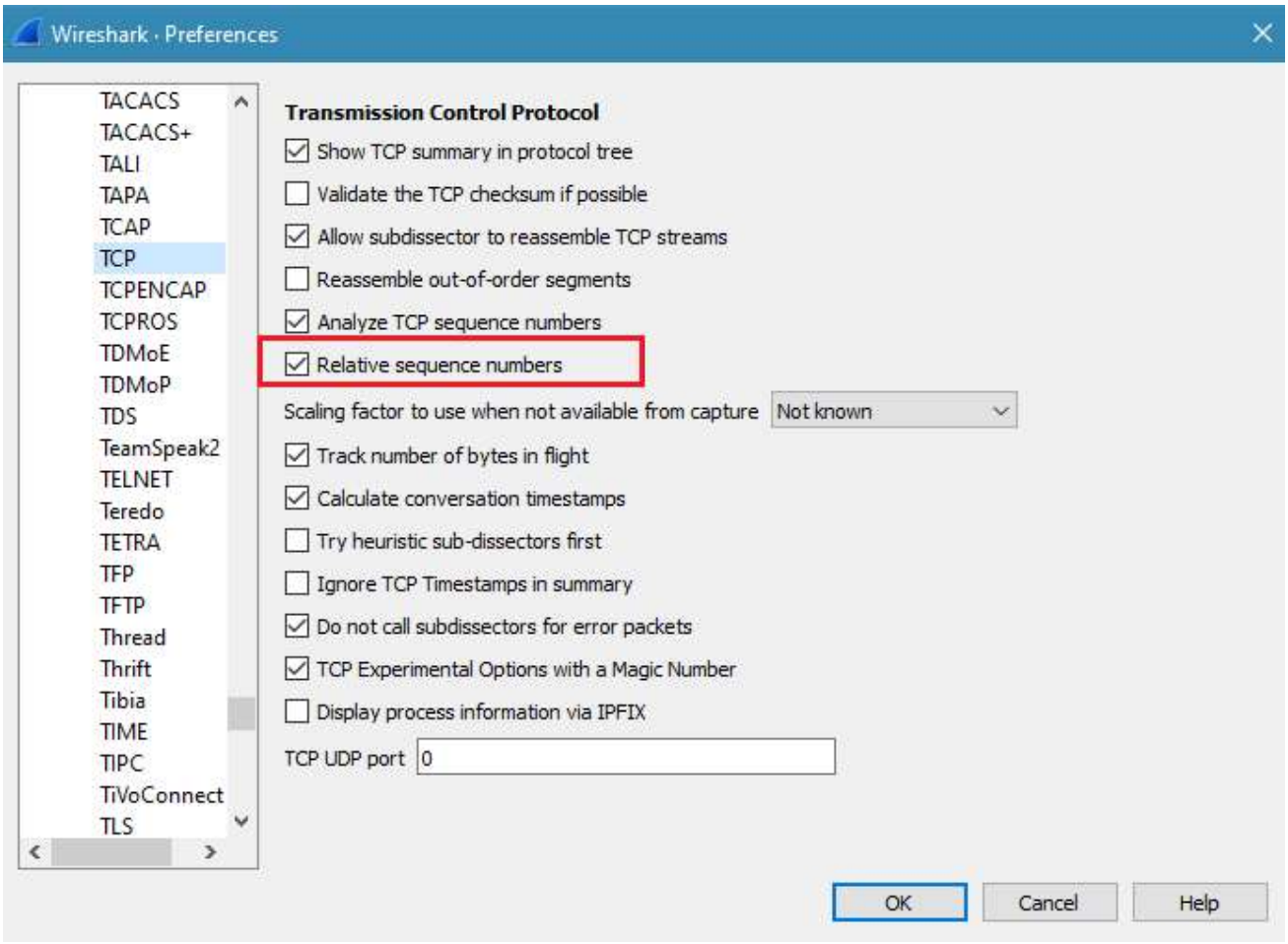
2.4. Quan sát các gói tin TCP

Sử dụng file lưu lượng ở mục 3.2 để quan sát và trả lời các câu hỏi.

- **Bước 1**: Trên menu của Wireshark, chọn **Analyze → Enabled Protocols**. Điền HTTP vào ô **Search** và bỏ chọn mục HTTP trong danh sách Protocol như hình dưới đây sau. Nhấn OK để đóng cửa sổ.



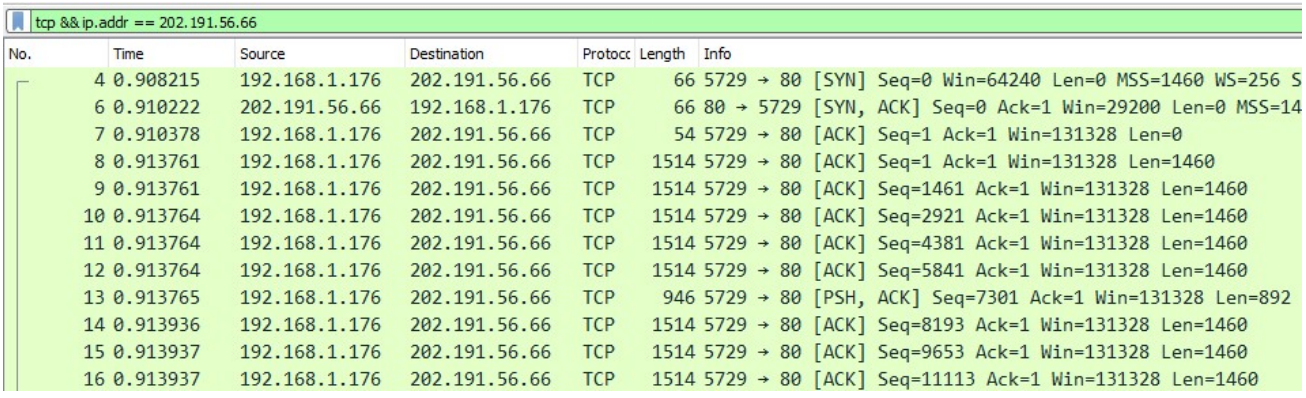
Trên menu của Wireshark, chọn **Edit → Preferences…** Trong mục **Protocol** của cửa sổ **Preference**, chọn **TCP**. Nhấn chọn mục **Relative sequence numbers** như hình sau:



- **Bước 2:** Điền giá trị sau vào mục Filter của Wireshark để lọc ra các gói tin TCP đã bắt được trong quá trình upload file.

tcp && ip.addr == 202.191.56.66

Hình dưới đây minh họa kết quả thực hiện:



- **Bước 3:** Tìm các gói tin được sử dụng để thiết lập liên kết giữa tiến trình Web Browser trên máy tính của sinh viên và máy chủ Web trong quá trình truy cập. Trả lời câu hỏi số 3

Câu hỏi 3(2 điểm): Địa chỉ của các bên trong liên kết là gì?

Địa chỉ IP bên khởi tạo …….. Địa chỉ IP bên đáp ứng:……..

Số hiệu cổng ứng dụng bên khởi tạo:……..

Số hiệu cổng ứng dụng bên đáp ứng:……..

Với mỗi gói tin trong quá trình thiết lập liên kết, hãy cho biết các thông số sau:

STT gói tin (No.)	*Giá trị **nhị phân** của trường Flags*	*Các cờ được thiết lập*	*Sequence number*	*ACK number*	*Kích thước phần dữ liệu*

- **Bước 4:** Tìm gói tin đầu tiên có chứa dữ liệu của file alice.txt đã upload và trả lời câu hỏi số 4. *(Gợi ý: Xem nội dung phần payload và so sánh với nội dung phần đầu file alice.txt)*

Câu hỏi 4(1 điểm): Xác định các thông số sau của gói tin

- *STT gói tin (No.):*
- *Địa chỉ IP nguồn:*
- *Địa chỉ IP đích:*
- *Số hiệu cổng nguồn:*
- *Số hiệu cổng đích:*
- *Sequence Number:*
- *ACK Number:*
- *Kích thước phần tiêu đề TCP:*
- *Kích thước phần dữ liệu:*
- *Các cờ được thiết lập:*
- *Gói tin này được đóng gói vào gói tin của giao thức tầng mạng nào?*

Hãy để ý rằng các thông số địa chỉ trên gói tin này có phù hợp với các thông số địa chỉ trong quá trình thiết lập liên kết hay không?

- **Bước 5:** Tìm gói tin báo nhận của Web Server cho gói tin đã quan sát ở bước 4 và trả lời câu hỏi số 5 và số 6.

Câu hỏi 5(2 điểm): Xác định các thông số sau của gói tin

- *STT gói tin (No.):*
- *Địa chỉ IP nguồn:*
- *Địa chỉ IP đích:*
- *Số hiệu cổng nguồn:*
- *Số hiệu cổng đích:*
- *Sequence Number:*
- *ACK Number:*
- *Kích thước phần tiêu đề TCP:*
- *Kích thước phần dữ liệu:*
- *Các cờ được thiết lập:*

Có thể kết luận chắc chắn Web Server đã nhận thành công gói tin ở bước 4 hay không? Tại sao?

Câu hỏi 6(2 điểm): Gói tin tiếp theo chứa dữ liệu của file được Web Browser gửi đi có giá trị Sequence Number là bao nhiêu?

Lưu ý: Kích thước phần dữ liệu trong gói tin quan sát được ở bước 4 có thể lớn hơn giá trị Maximum Segment Size theo lý thuyết của giao thức TCP. Đó là do hệ đều hành kích hoạt cơ chế TCP Large Segment Offload.

- **Bước 6:** Tìm các gói tin được sử dụng để đóng liên kết TCP đã thiết lập và trả lời câu hỏi số 7.

Lưu ý: Nếu không tìm thấy đầy đủ các gói tin TCP để đóng liên kết, có thể trình duyệt duy trì liên kết lâu hơn. Sinh viên nên thực hiện lại thao tác bắt gói tin của mục 3.2 và chờ khoảng thời gian lâu hơn trong bước 8.

Câu hỏi 7(2 điểm): Với mỗi gói tin trong quá trình đóng liên kết, hãy cho biết các thông số sau:

STT gói tin (No.)	*Giá trị **nhị phân** của trường Flags*	*Các cờ được thiết lập*	*Sequence number*	*ACK number*	*Kích thước phần dữ liệu*