Mạng máy tính căn bản

Bài thực hành số 05

Tìm hiểu TCP, UDP với Wireshark

Họ tên: .....
MSSV: ..... Nhóm: .....

I. Mục tiêu:

- Tìm hiểu hành vi của TCP, UDP trong thực tế.
- Phân tích các gói tin của các phân đoạn TCP, UDP dùng để gửi và nhận một tập tin từ máy tính của bạn đến một máy chủ từ xa.
- Tìm hiểu cách TCP sử dụng số thứ tự (sequence number) và số xác nhận (acknowledgement number) để cung cấp dịch vụ truyền dữ liệu đáng tin cậy.

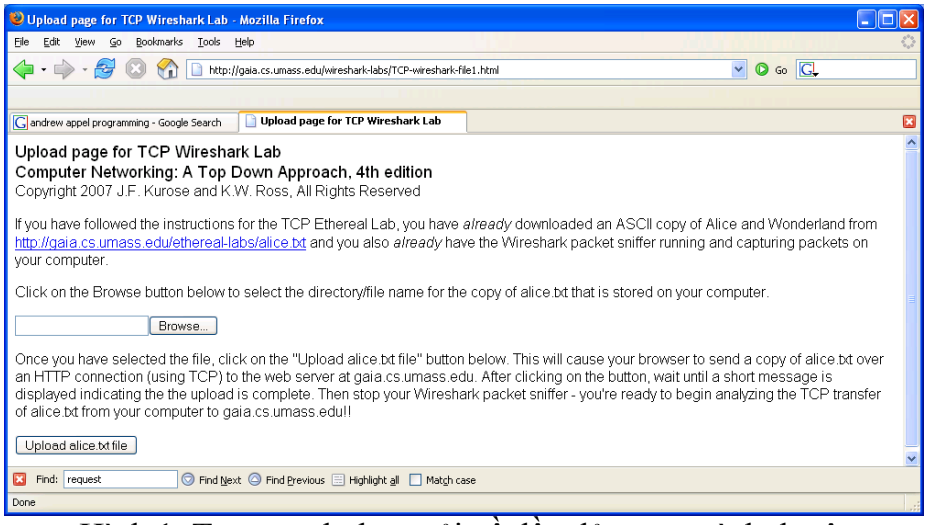
II. Nội dung

1. Bắt một số lượng lớn gói tin TCP chuyển từ máy tính của bạn đến một máy chủ từ xa

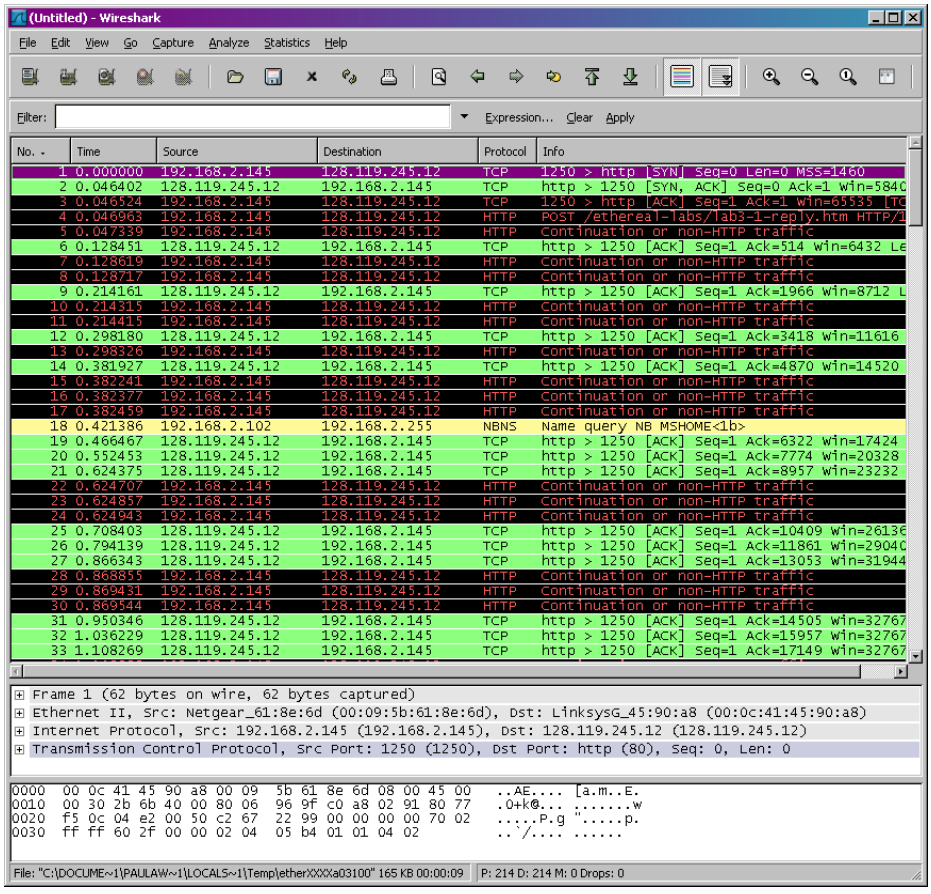
Sử dụng Wireshark để bắt được các gói TCP của một tập tin gửi từ máy tính của bạn đến một máy chủ từ xa. Ta sẽ tiến hành upload một file lên mạng và sử dụng Wireshark để bắt các gói tin trong quá trình này.

Các bước thực hiện:

- Khởi động trình duyệt web của bạn. truy cập tới http://gaia.cs.umass.edu/wireshark-labs/alice.txt và lấy một bản sao ASCII của "Alice in Wonderland". Lưu trữ tập tin một nơi nào đó trên máy tính của bạn.
- Tiếp đến vào trang http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html .
- Bạn sẽ thấy một màn hình trông giống như hình 1.
- Sử dụng nút Browse trong trang này để nhập vào tên của tập tin (tên đường dẫn đầy đủ) trên máy tính của bạn có chứa "Alice in Wonderland".
- Bây giờ khởi động Wireshark và bắt đầu bắt gói tin (Capture-> Start).
- Quay trở lại trình duyệt của bạn, nhấn vào nút "Upload alice.txt file" để tải lên các tập tin đến máy chủ gaia.cs.umass.edu. Một khi tập tin đã được tải lên một đoạn tin thông báo chúc mừng ngắn sẽ được hiển thị trong cửa sổ trình duyệt của bạn.
- Dừng bắt gói tin Wireshark. Cửa sổ Wireshark của bạn sẽ trông tương tự như cửa sổ hiển thị như hình 2.

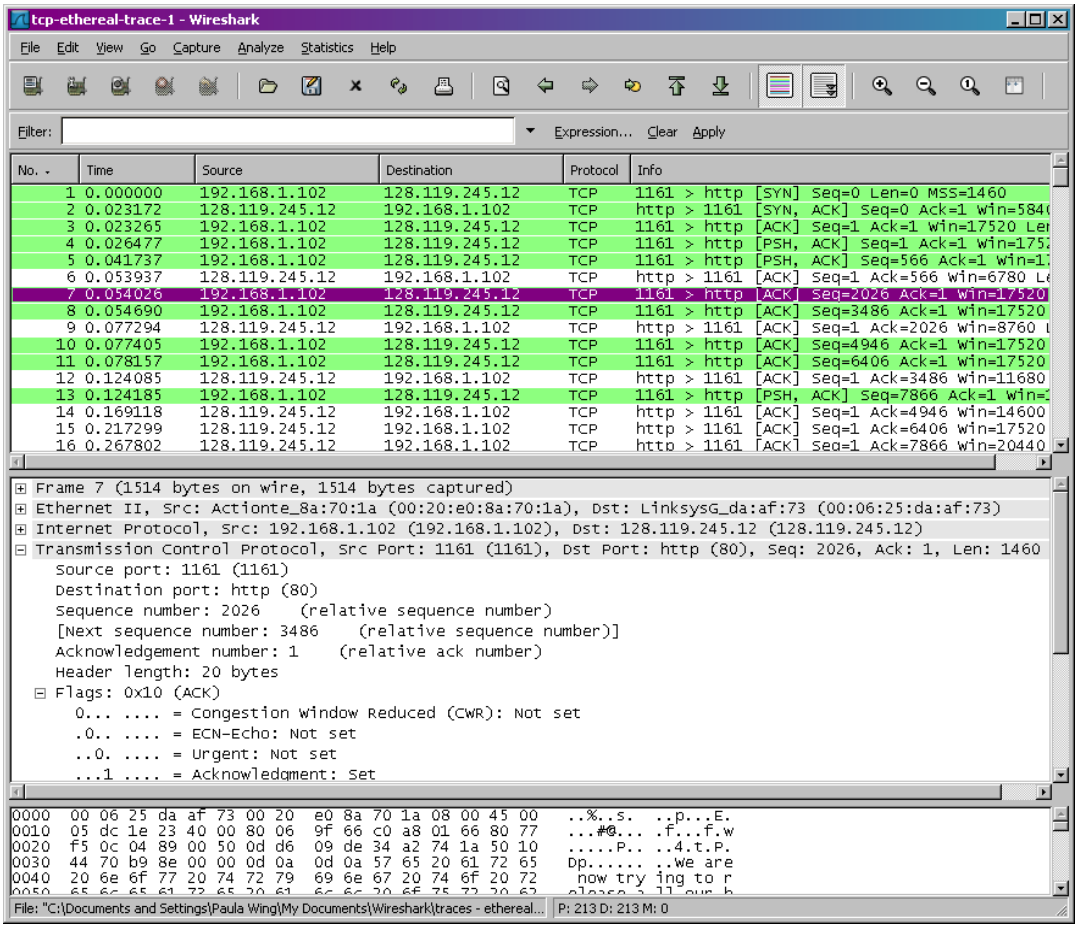


Hình 1. Trang web được tải về đầy đủ trong trình duyệt



Hình 2. Cửa sổ Wireshark sau khi bắt gói

Nếu bạn không thể chạy Wireshark trên một mạng kết nối trực tiếp, bạn có thể tải về một gói các tập tin đã được bắt trong khi thực các bước trên. Để hiển thị thông tin về các phân đoạn TCP từ thanh công cụ Analyze-> Enabled Protocols. Sau đó bỏ chọn hộp HTTP và chọn OK. Bây giờ bạn sẽ thấy một cửa sổ Wireshark trông giống như hình 3.



Hình 3. Cửa sổ wireshark sau khi bỏ chọn giao thức HTTP

2. Phân tích gói tin TCP

Trước khi phân tích hành vi của các kết nối TCP cụ thể, chúng ta hãy có một cái nhìn tổng quát về các gói tin. Đầu tiên, bộ lọc gói tin hiển thị trong cửa sổ Wireshark bằng cách nhập vào "tcp" (chữ thường, không có dấu ngoặc kép, và không quên nhấn Enter sau khi nhập) vào bộ lọc nằm phía trên của cửa sổ Wireshark.

Những gì bạn sẽ thấy là hàng loạt thông điệp TCP và HTTP giữa các máy tính của bạn và gaia.cs.umass.edu.Bạn sẽ thấy thông điệp:

- Bắt tay ba chiều đầu tiên có chứa một thông điệp SYN. Bạn sẽ thấy một thông báo HTTP POST.
- Các thông điệp "HTTP continuation" được gửi đi từ máy tính của bạn đến gaia.cs.umass.edu.
- Các phân đoạn TCP ACK được trả lại từ gaia.cs.umass.edu tới máy tính của bạn.

Lưu ý: Trong bài thực hành HTTP với wireshark không có kiểu thông điệp "HTTP continuation" - đây là cách mà Wireshark chỉ ra rằng có nhiều phân đoạn TCP đang được sử dụng để mang một thông điệp HTTP duy nhất.

Trả lời các câu hỏi sau bằng cách mở tập tin gói tin Wireshark trong các gói tin nhận được:

1. Địa chỉ IP và số cổng TCP được sử dụng bởi máy tính khách (source) khi chuyển tập tin đến gaia.cs.umass.edu là gì?

2. Địa chỉ IP của gaia.cs.umass.edu là gì? Các phân đoạn TCP của kết nối này được gửi và nhận trên cổng bao nhiêu?

3. Số thứ tự của phân đoạn TCP SYN được sử dụng để khởi tạo kết nối TCP giữa các máy tính khách hàng và gaia.cs.umass.edu là gì? Trong phân đoạn, trường nào chỉ ra rằng đó là một phân đoạn SYN?

4. Số thứ tự của đoạn SYNACK được gửi bởi gaia.cs.umass.edu vào máy tính của khách hàng để trả lời cho đoạn SYN là gì? Giá trị của trường ACK trong phân đoạn SYNACK là gì? Làm thế nào gaia.cs.umass.edu xác định giá trị đó? Trường nào trong phân đoạn đó chỉ ra nó là một phân đoạn SYNACK?

5. Chiều dài của phân mỗi trong sáu phân đoạn TCP đầu tiên là bao nhiêu?

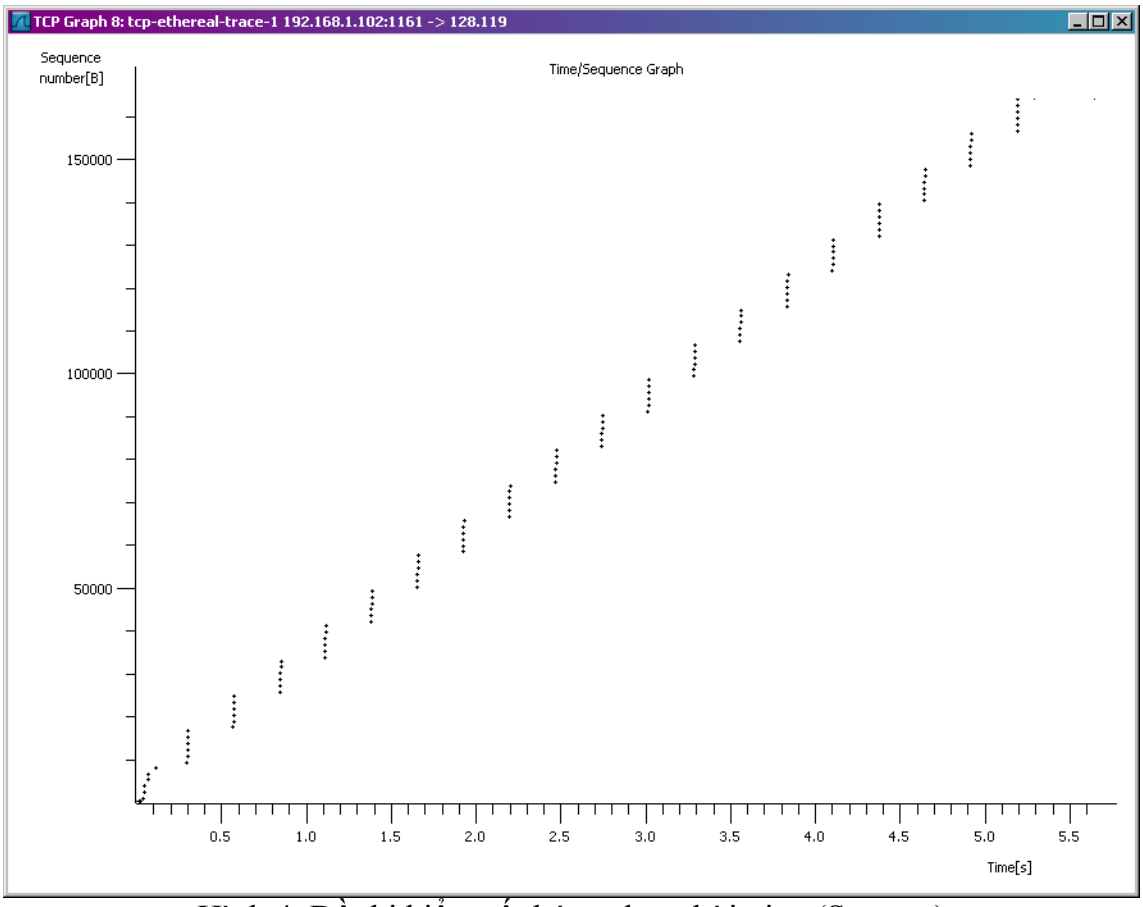
6. Số khoảng trống trong bộ nhớ đệm nhỏ nhất của được quảng bá cho người nhận trong toàn bộ quá trình là bao nhiêu? Sự thiếu bộ nhớ đệm bên nhận có khi nào điều chỉnh tốc độ của người gửi không?

7. Có bất kỳ phân đoạn được truyền lại không? Bạn phải kiểm tra (trong các gói tin bắt được) để trả lời câu hỏi này.

4. Giải thuật kiểm soát tắc nghẽn TCP trong thực tế

Bây giờ chúng ta hãy xem xét số lượng dữ liệu được gửi đi mỗi đơn vị thời gian từ khách hàng để máy chủ. Thay vì tính toán từ các dữ liệu thô trong cửa sổ Wireshark, chúng ta sẽ sử dụng một trong những tiện ích của giao thức TCP Wireshark - đồ thị (Stevens) để vẽ ra dữ liệu.

Chọn một phân đoạn TCP trong "danh sách bắt các gói tin" cửa sổ của Wireshark.
Sau đó chọn menu: Statistics-> TCP Stream Graph-> Time-Sequence Graph (Stevens). Bạn sẽ thấy một đồ thị trông tương tự như đồ thị ở hình 4 sau đây.



Hình 4. Đồ thị kiểm số thứ tự theo thời gian (Stevens)

Ở đây, mỗi chấm đại diện cho một phân đoạn TCP gửi đi, thể hiện số thứ tự của phân đoạn này so với thời gian mà tại đó nó được gửi đi. Lưu ý rằng một tập hợp các dấu chấm được xếp chồng lên nhau trên nhau đại diện cho một loạt các gói dữ liệu được gửi liên tục (back-to-back) bởi người gửi.

5. Bắt gói tin UDP

Cũng tương tự như bắt gói tin TCP. Trong bộ lọc của Wireshark nhập vào UDP để lọc và tìm gói tin UDP. Chọn một gói tin UDP và trả lời các câu hỏi sau:

1. Chọn một gói tin. Từ gói tin này, xác định có bao nhiêu trường trong nào đầu UDP. (Xem trong sách giáo khoa và trả lời những câu hỏi trực tiếp từ những gì bạn quan sát ở các gói tin.) Tên các trường này.

2. Từ trường nội dung gói tin, xác định độ dài (byte) của mỗi trường trong mào đầu của UDP.

3. Giá trị trong trường Length là chiều dài của cái gì? Kiểm tra thông tin này với gói tin UDP bạn bắt được.

4. Tìm kiếm "UDP" bằng Google và xác định các trường mà được tính trong tổng kiểm tra (checksum) UDP.