BÀI TẬP THỰC HÀNH SỐ 3
MÔN HỌC: NHẬP MÔN MẠNG MÁY TÍNH

TCP VÀ UDP

1 Mục tiêu

- Tìm hiểu về hành vi của TCP và UDP.
- Phân tích quá trình gửi và nhận một file 150KB từ máy khách lên máy chủ.
- Tìm hiểu việc TCP sử dụng sequence number và acknowledgement number để có thể truyền dữ liệu tin cậy.

2 Bắt gói và phân tích UDP

- Bật Wireshark, bắt đầu bắt gói. Thông thường sẽ xuất hiện một số gói tin UDP như SNMP sẽ xuất hiện trên danh sách các gói tin.
- Ngưng bắt gói, lọc các gói tin UDP để Wireshark chỉ hiển thị các gói tin UDP. Nếu không có gói tin UDP nào thì chúng ta cũng có thể sử dụng file htp-ethereal-trace-5 đã được cung cấp trong thư mục wireshark-traces.

Trả lời các câu hỏi sau:

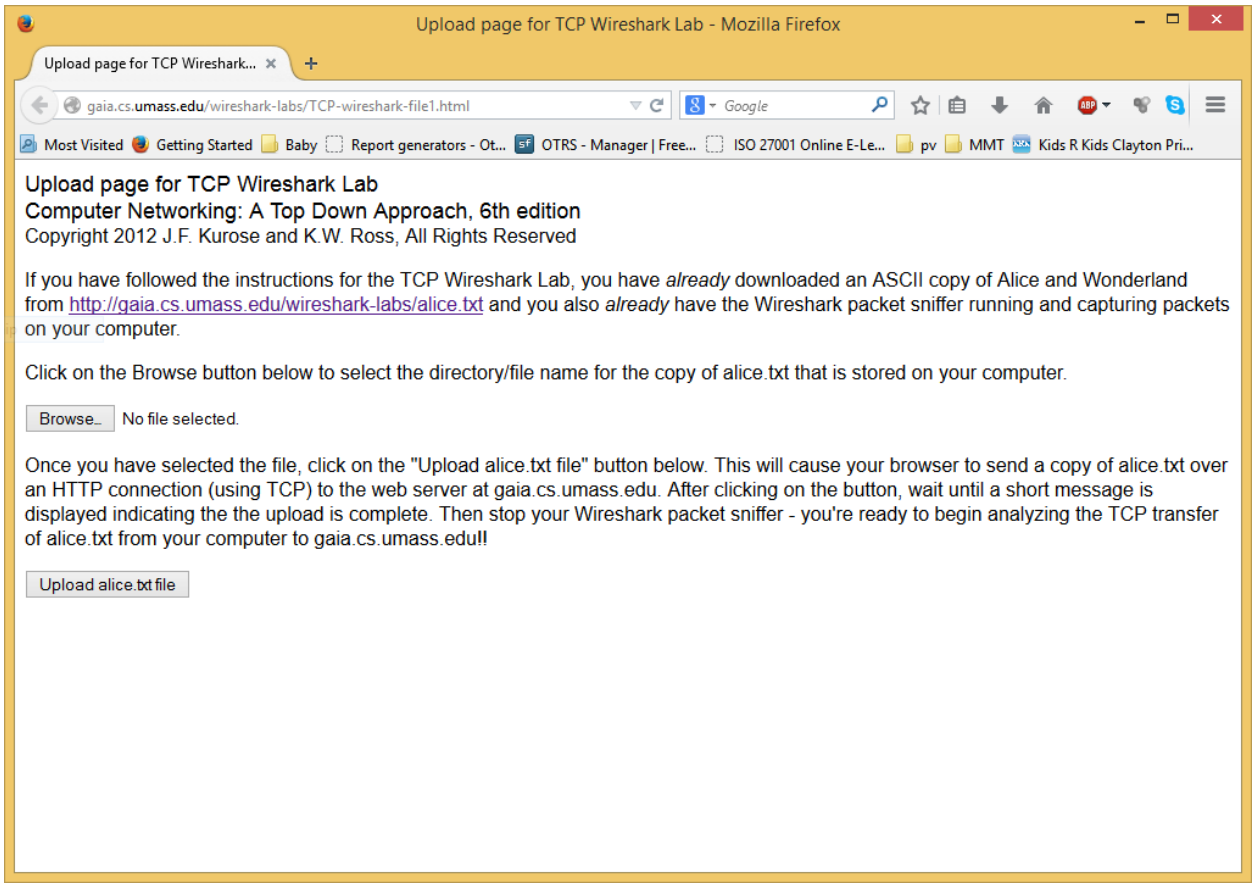
1. Chọn một gói tin UDP, xác định các trường (field) trong UDP header?
2. Qua thông tin hiển thị của Wireshark, xác định độ dài (tính theo byte) của mỗi trường trong UDP header?
3. Giá trị của trường Length là độ dài của cái gì? Chứng minh?
4. Số bytes lớn nhất mà payload của UDP có thể chứa?
5. Giá trị lớn nhất có thể có của port nguồn?
6. Xác định protocol number của UDP (cả hệ 10 lẫn hệ 16)? Để trả lời câu hỏi này, chúng ta cần phải xem trường Protocol của IP header.

3 Bắt gói tin trong quá trình gửi file sử dụng TCP lên máy chủ

Chú ý: nếu chúng ta không thể chạy Wireshark trên Internet thật sự thì có thể mở file tcp-ethereal-trace-1 có sẵn trong thư mục wireshark-traces.

Thực hiện các bước sau khi có kết nối Internet:

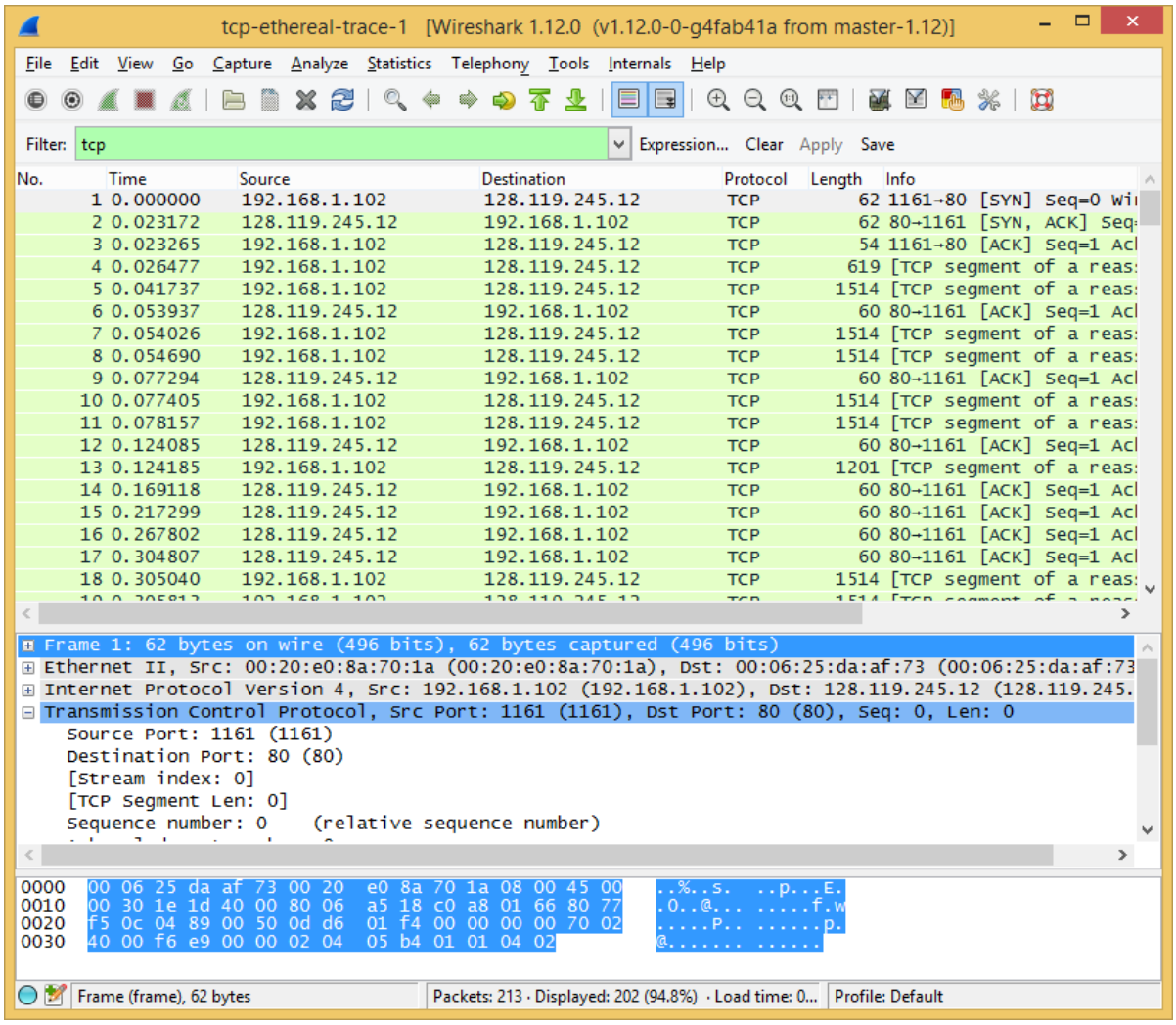
- Mở trình duyệt. Truy cập trang http://gaia.cs.umass.edu/wireshark-labs/alice.txt và lưu file vào máy tính.
- Truy cập trang http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html



- Sử dụng nút ***Browse*** trong trang web để chọn file alice.txt vừa download. Đừng nhấn nút ***Upload alice.txt file***
- Mở Wireshark và bắt đầu bắt gói (Capture -> Start).
- Quay lại trình duyệt, nhấn nút ***Upload alice.txt file*** để upload file lên server. Khi file đã được upload, một tin nhắn chúc mừng sẽ xuất hiện trên trình duyệt.
- Ngưng bắt gói

4 Phân tích hành vi TCP

- Gõ "tcp" vào bộ lọc của Wireshark để hiển thị tất cả các gói tin TCP.



Quan sát các gói tin và trả lời các câu hỏi sau: (để có minh chứng cho câu trả lời, chúng ta cần chụp lại màn hình hoặc dùng chức năng "***Print***" của Wireshark: File -> Print Chọn ***Selected packet only*** và ***Packet summary line***).

7. Tìm địa chỉ IP và TCP port của máy khách gửi file cho gaia.cs.umass.edu?
8. Tìm địa chỉ IP của gaia.cs.umass.edu? Kết nối TCP dùng để gửi và nhận các segments sử dụng port nào?
9. TCP SYN segment sử dụng sequence number nào để khởi tạo kết nối TCP giữa máy khách và gaia.cs.umass.edu? Thành phần nào trong segment cho ta biết segment đó là TCP SYN segment?

10. Tìm sequence number của SYNACK segment được gửi bởi gaia.cs.umass.edu đến máy khách để trả lời cho SYN segment? Tìm giá trị của Acknowledgement trong SYNACK segment? Làm sao gaia.cs.umass.edu có thể xác định giá trị đó? Thành phần nào trong segment cho ta biết segment đó là SYNACK segment?
11. Tìm sequence number của TCP segment có chứa lệnh HTTP POST?