BÀI TẬP LỚN NHỎ (MINI-PROJECT)

Chủ đề: Phân tích hành trình kết nối Web bằng phần mềm Wireshark
Textbook: *Computer Networking: A Top-Down Approach (Kurose & Ross)* — Chapters 1, 2, 3
Thời gian thực hiện: 01 đến 02 tuần

1. MỤC TIÊU BÀI TẬP

Sau khi hoàn thành bài tập này, sinh viên có khả năng:

- Sử dụng thành thạo công cụ **Wireshark** để bắt và lọc gói tin theo giao thức/địa chỉ IP.
- Phân tích và giải thích cách vận hành của **DNS** và **HTTP/HTTPS** ở Tầng ứng dụng (*Chapter 2*).
- Quan sát, giải mã quá trình bắt tay 3 bước (**TCP 3-Way Handshake**) và cơ chế điều khiển luồng của TCP ở Tầng giao vận (*Chapter 3*).
- Đo lường các thông số hiệu năng thực tế như **RTT (Round Trip Time)** ở Tầng mạng (*Chapter 1*).

2. CHUẨN BỊ & DỤNG CỤ

1. **Phần mềm:** Cài đặt Wireshark (phiên bản mới nhất) tại wireshark.org.
2. **Môi trường:** Máy tính cá nhân kết nối Internet (Wi-Fi hoặc cáp Ethernet).
3. **Trình duyệt:** Chrome / Firefox / Edge (khuyến khích dùng chế độ Ẩn danh / Incognito).

3. KỊCH BẢN THỰC HIỆN

Bước 1: Xóa bộ nhớ đệm DNS (DNS Cache)

Để đảm bảo máy tính bắt buộc phải gửi truy vấn DNS mới ra ngoài Internet, sinh viên thực hiện theo thứ tự sau:

1. Đóng toàn bộ các cửa sổ/tab trình duyệt đang mở để xóa triệt để bộ nhớ đệm DNS nội bộ của trình duyệt.
2. Xóa DNS cache của Hệ điều hành:
    - **Windows:** Mở CMD (quyền Admin) $\rightarrow$ gõ lệnh: ipconfig /flushdns
    - **macOS:** Mở Terminal $\rightarrow$ gõ lệnh: sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder
3. Mở lại trình duyệt ở chế độ ẩn danh (Incognito / Private mode) để chuẩn bị bắt gói tin.

Bước 2: Bắt gói tin trên Wireshark

1. Mở Wireshark, chọn Card mạng đang kết nối Internet (ví dụ: Wi-Fi hoặc Ethernet) và nhấn biểu tượng **Start Capture** (hình vây cá đuối màu xanh).
2. Mở trình duyệt ở chế độ ẩn danh, truy cập vào một trang web sử dụng giao thức HTTP chưa mã hóa do giảng viên chỉ định.
    - **Lưu ý quan trọng:** Khi gõ địa chỉ, sinh viên **bắt buộc phải gõ đầy đủ tiền tố http://** (ví dụ: http://neverssl.com).
    - Nếu trình duyệt tự động chuyển hướng sang https://, sinh viên hãy thử truy cập các trang web dự phòng sau: http://httpbin.org/get hoặc http://example.com.
3. Ngay khi trang web tải xong, quay lại Wireshark và nhấn **Stop Capture** (nút vuông màu đỏ).
4. Lưu file dữ liệu vừa bắt được thành file .pcapng với tên: **[MSSV]_[HoTen]_LabWireshark.pcapng**

4. CÁC CÂU HỎI & YÊU CẦU PHÂN TÍCH

Sinh viên trả lời đầy đủ các câu hỏi dưới đây vào báo cáo, kèm hình chụp màn hình minh chứng từ Wireshark.

PHẦN 1: PHÂN TÍCH TẦNG ỨNG DỤNG (APPLICATION LAYER - CHAPTER 2)

1.1. Giao thức DNS

- **Filter:** Gõ dns vào thanh lọc của Wireshark.
- **Câu hỏi:**
    1. Tìm gói tin *DNS Query* gửi đi và *DNS Response* trả về cho tên miền trang web bạn truy cập.
    2. Mã **Transaction ID** của truy vấn DNS này là bao nhiêu?
    3. Địa chỉ IP của Web Server được phản hồi trong gói *DNS Response* là gì?
    4. DNS sử dụng giao thức tầng giao vận nào (TCP hay UDP)? Giải thích ngắn gọn lý do tại sao lại dùng giao thức đó trong trường hợp này.

1.2. Giao thức HTTP

- **Filter:** Gõ http vào thanh lọc. *(Lưu ý: Nếu không xuất hiện gói tin HTTP nào, kiểm tra xem trình duyệt có bị tự động chuyển sang HTTPS/TLS hay không)*.
- **Câu hỏi:**
    1. Tìm gói tin request GET / HTTP/1.1.
    2. Xác định các trường Header sau trong gói GET request: User-Agent, Host, Accept-Language.
    3. Mã trạng thái (Status Code) và thông điệp trả về trong gói HTTP Response từ Server là gì (ví dụ: 200 OK, 301 Moved Permanently)? Nêu ngắn gọn ý nghĩa của mã trạng thái đó.

PHẦN 2: PHÂN TÍCH TẦNG GIAO VẬN (TRANSPORT LAYER - CHAPTER 3)

2.1. Quá trình bắt tay 3 bước của TCP (TCP 3-Way Handshake)

- **Filter:** Gõ ip.addr == <Địa_chỉ_IP_Server> (thay <Địa_chỉ_IP_Server> bằng IP tìm được ở Phần 1.1).
- **Câu hỏi:**
    1. Xác định 3 gói tin thực hiện quá trình bắt tay 3 bước (SYN, SYN-ACK, ACK). Chụp lại màn hình rõ 3 gói tin này.
    2. Ghi lại các thông số sau của từng gói tin trong 3-way handshake:
        - **Cổng nguồn (Source Port)** và **Cổng đích (Destination Port)**.
        - Giá trị **Sequence Number (Seq)** và **Acknowledgment Number (Ack)** thực tế (Raw) cũng như giá trị tương đối (Relative).
    3. Giải thích ngắn gọn quy luật tăng chỉ số Seq và Ack qua từng bước của quá trình bắt tay.

2.2. Điều khiển luồng (Flow Control) & Kích thước cửa sổ

- **Câu hỏi:**
    1. Kích thước cửa sổ nhận (**Receive Window Size - win**) được khai báo bởi Client (trong gói SYN) và Server (trong gói SYN-ACK) là bao nhiêu byte?
    2. Kích thước cửa sổ này có vai trò gì trong việc kiểm soát luồng dữ liệu giữa Client và Server?

PHẦN 3: TỔNG QUAN HỆ THỐNG & ĐO LƯỜNG HIỆU NĂNG (CHAPTER 1)

3.1. Tính toán thời gian khứ hồi RTT (Round Trip Time)

Câu hỏi:

- Dựa vào cột thời gian (**Time**) trên Wireshark, hãy tính thời gian RTT giữa Client và Server dựa trên gói bắt tay TCP bằng công thức (Timestamp lấy tại Client):

    RTT= Timestamp(gói SYN-ACK)-Timestamp(gói SYN)
- Thực hiện lệnh ping <Địa_chỉ_IP_Server> trong Terminal/CMD để kiểm tra thời gian RTT thực tế qua ICMP. So sánh giá trị RTT thu được từ Ping với giá trị RTT tính bằng Wireshark ở trên.
- **Xử lý tình huống mở:** Nếu lệnh ping báo Request timed out (không nhận được phản hồi), hãy cho biết nguyên nhân tại sao lại xảy ra hiện tượng này và tại sao quá trình TCP Handshake trên Wireshark vẫn diễn ra bình thường?

3.2. Sơ đồ luồng dữ liệu (Flow Graph)

- **Yêu cầu:**
    1. Vào menu Statistics Flow Graph.
    2. Chọn *Flow type:* TCP Flows.
    3. Xuất hình ảnh sơ đồ luồng trao đổi dữ liệu từ bước khởi tạo TCP cho đến khi truyền dữ liệu HTTP. Chèn hình ảnh này vào báo cáo.

5. QUY ĐỊNH NỘP BÀI & TIÊU CHÍ ĐÁNH GIÁ

5.1. Nộp bài **- nộp quyển** và 01 file nén (.zip hoặc .rar) đặt tên: [MSSV]_[HoTen]_MiniProject.zip bao gồm:

- BaoCao_[MSSV].pdf: File báo cáo trả lời đầy đủ các câu hỏi ở Mục 4. Mỗi câu trả lời **bắt buộc phải có hình ảnh chụp màn hình Wireshark tương ứng** (khoanh vùng chi tiết thông tin cần chỉ ra).
- Capture_[MSSV].pcapng: File dữ liệu thô do sinh viên tự bắt được trên máy của mình.

5.2. Thang điểm đánh giá (Rubric)

Hạng mục	Tiêu chí đánh giá	Trọng số
Phần 1: Application Layer	Lọc đúng gói tin DNS/HTTP; trả lời chính xác thông số Header, Status Code, IP Server.	**30%**
Phần 2: Transport Layer	Chỉ rõ 3-way handshake; phân tích đúng quy luật Seq/Ack và Window Size.	**40%**
Phần 3: Performance & Flow	Tính toán chính xác RTT; xuất đúng sơ đồ Flow Graph.	**20%**
Hình thức & File PCAP	File .pcapng hợp lệ (khớp với hình ảnh báo cáo); báo cáo trình bày rõ ràng, mạch lạc.	**10%**

LƯU Ý: Bài làm phát hiện trùng lặp file .pcapng hoặc sao chép hình ảnh báo cáo của nhau sẽ nhận điểm 0 cho cả hai bài.