BÀI TẬP THỰC HÀNH BẢO MẬT MẠNG MÁY TÍNH VÀ HTTT

Làm quen với Wireshark

Họ và tên: Nguyễn Thanh Trường

Lớp: 10\_ĐH\_CNPM1

MSSV: 1050080082

**Task 1: Mở đầu về Mạng máy tính**

* Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).
  + Router (bộ định tuyến)
  + Switch(Bộ chuyển mạch)
  + Modem
  + Firewall

- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

- Gián đoạn công việc trực tuyến

- Không truy cập được các tài liệu trực tuyến (GG drive, OneDrive,....)

- Không thể giải trí trực tuyến (xem phim, nghe nhạc, chơi game online,...)

- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

- Hiểu được các khái niệm cơ bản về mạng máy tính

- Biết được cách thiết lập, cấu hình thiết bị mạng cơ bản

- Hiểu về các giao thức mạng

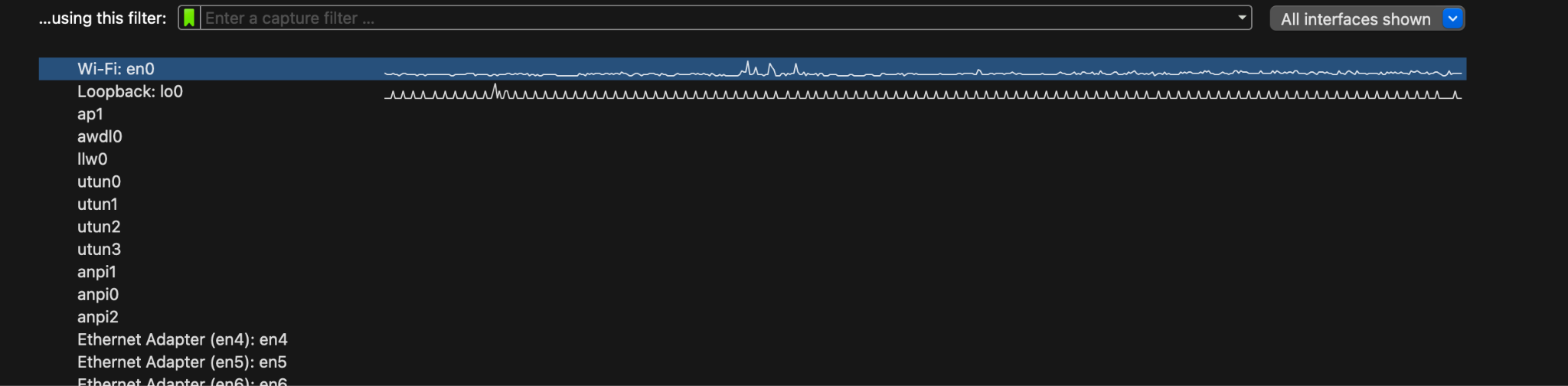
- Nắm được cách bảo mật mạng và khắc phục sự cố mạng cơ bản

- Có khả năng ứng dụng kiến thức để thiết kế, triển khai một hệ thống mạng nhỏ

**Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng**

Bước 1: Khởi động trình duyệt web bất kỳ như Google Chrome, Firefox, Edge,...và phần mềm Wireshark (phiên bản mới nhất)

Bước 2 : Tại phần Capture, chọn interface đang hoạt động chính trên máy để bắt đầu bắt gói tin.

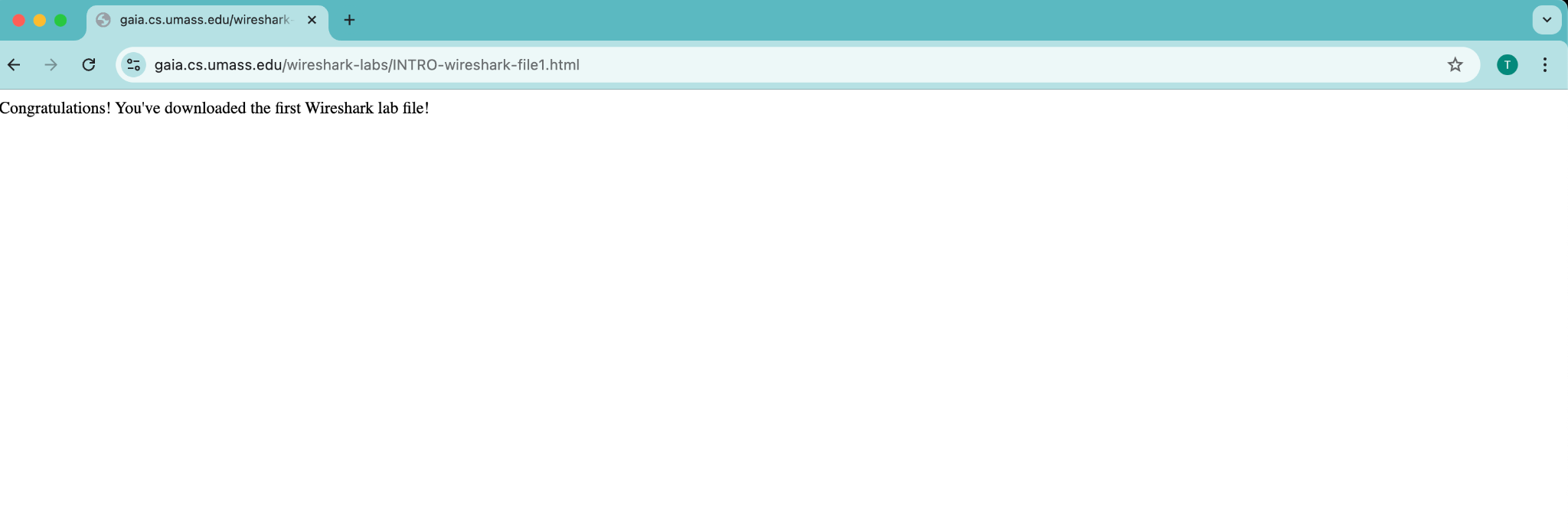


Bước 3: Sau đó, cửa sổ như Hình trên sẽ xuất hiện và hiển thị kết quả bắt gói tin tại interface đã chọn.

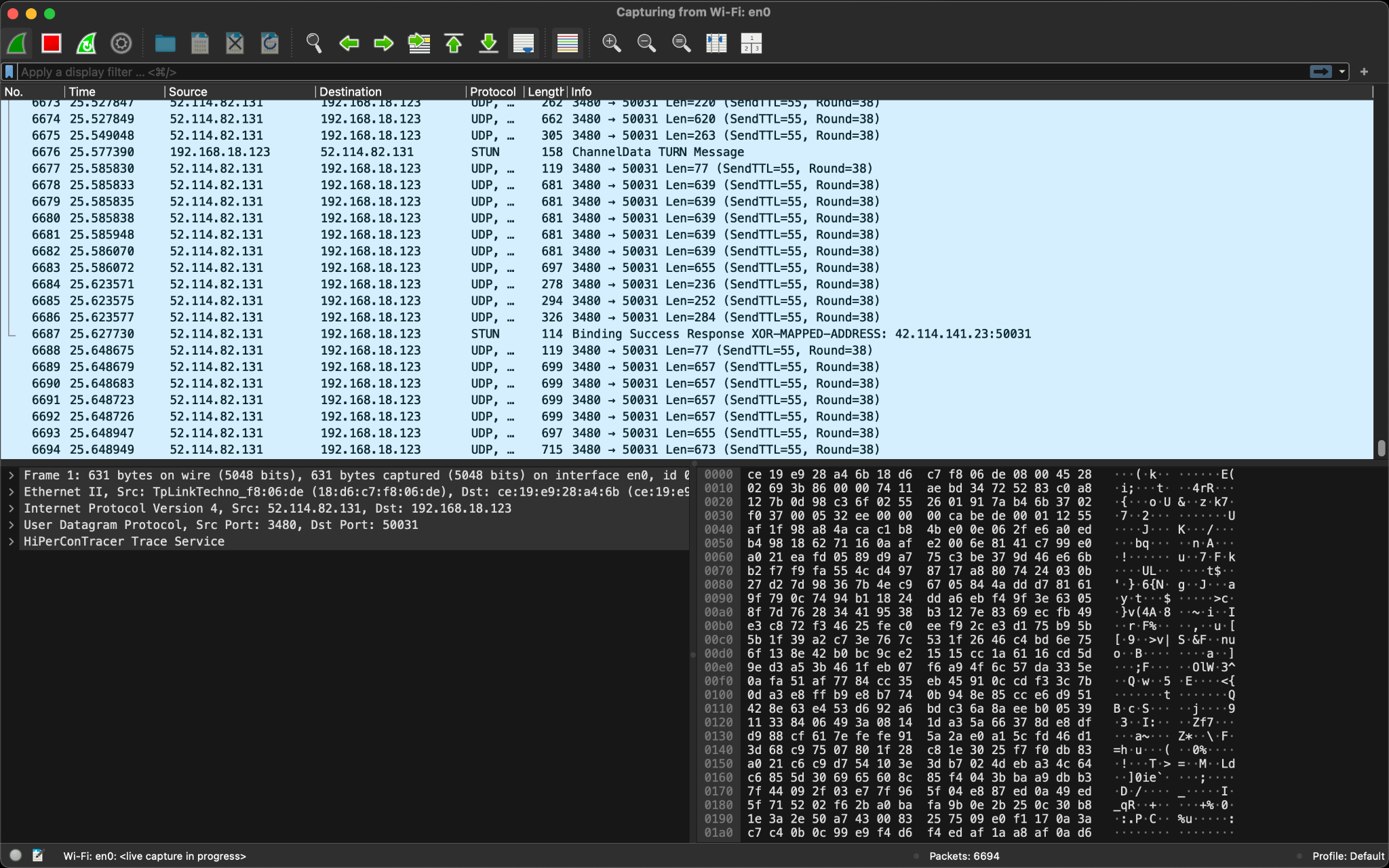
Bước 4: Mở trình duyệt web và chỉ truy cập vào website có địa chỉ như sau

<http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

Đây là một website đơn giản có nội dung như sau:



Bước 5: Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.



Cửa sổ chính của Wireshark bây giờ giống như Hình 7. Bạn đã có các gói tin

chứa đầy đủ các thông điệp được trao đổi giữa máy tính và web server. Thông

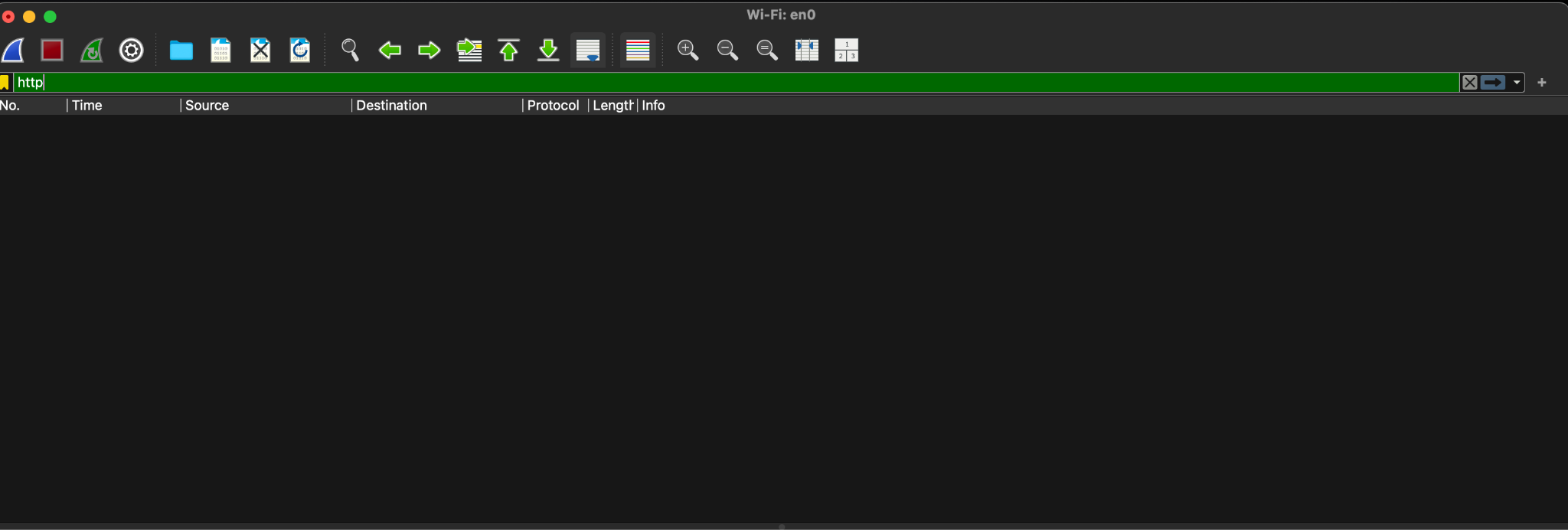
điệp HTTP trao đổi với web server gaia.cs.umass.edu phải xuất hiện đâu đó

trong các gói tin được bắt.

Có nhiều loại gói tin được hiển thị (tương ứng với nhiều giao thức). Mặc dù bạn

chỉ đơn thuần truy cập một trang web nhưng cũng có nhiều giao thức khác chạy bên dưới mà bạn không thấy được.

Bước 6: Gõ “http” vào packet-display filter sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window.



Bước 7: Tìm 2 thông điệp HTTP GET được gửi từ máy tính đến gaia.cs.umass.edu server (tìm trong packet-listing window đoạn chứa GET theo sau bởi gaia.cs.umass.edu) và HTTP 200 OK được trả về từ server đến máy tính hiện tại. Sau khi chọn thông điệp HTTP GET, các thông tin về Ethernet frame, IP datagram, TCP segment và HTTP header sẽ được hiển thị ở packet-header window.

Bước 8: Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng

MSSV-Bai1.pcapng. Ví dụ: 18521006-Bai1.pcapng.

Bước 9: Chọn biểu tượng Start capturing packets để bắt đầu quá trình bắt gói tin mới.

Bước 10: Chọn 1 website mà sinh viên thường hay truy cập, ví dụ uit.edu.vn,

tinhte.vn,... và tiến hành bắt gói tin trên website đó

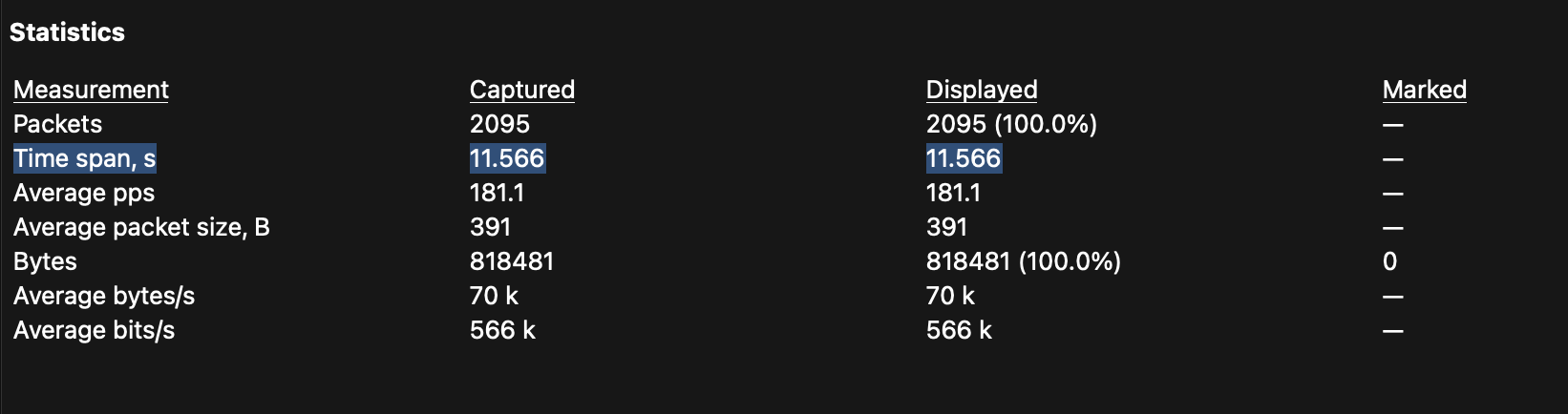
Lặp lại các bước 4-5-6-7 với một website khác có chứa nhiều thông tin hơn mà sinh viên thường truy cập. Ví dụ: tuoitre.vn, uit.edu.vn,...

Bước 11: Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên dạng MSSV-Bai2.pcapng

**2.3Phân tích kết quả bắt gói tin từ Wireshark**

**1. Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?**

* Tổng thời gian là 11.566s

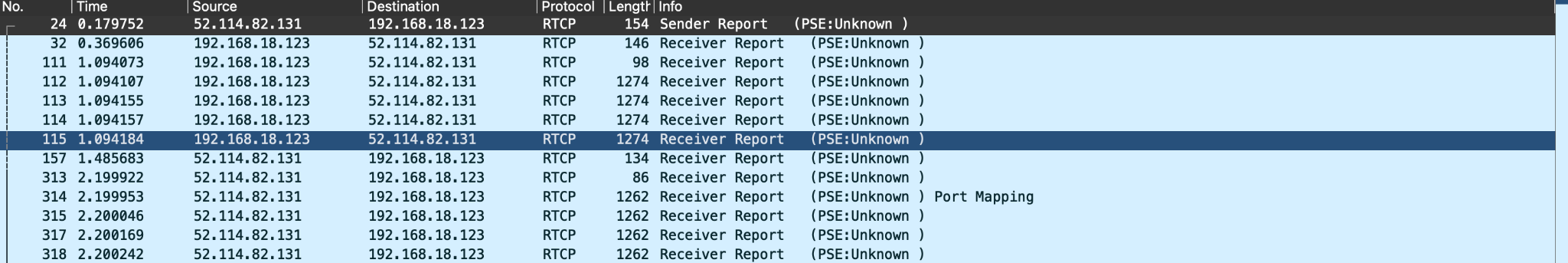


**2. Liệt kê ít nhất 5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol)khi không áp dụng bộ lọc “http” khi truy cập 2 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.**

1. RTCP (RTP Control Protocol)

Chức năng: Hỗ trợ RTP (Real-time Transport Protocol) bằng cách cung cấp thông tin về chất lượng truyền tải, độ trễ và jitter trong truyền tải dữ liệu thời gian thực như cuộc gọi VoIP, video call.

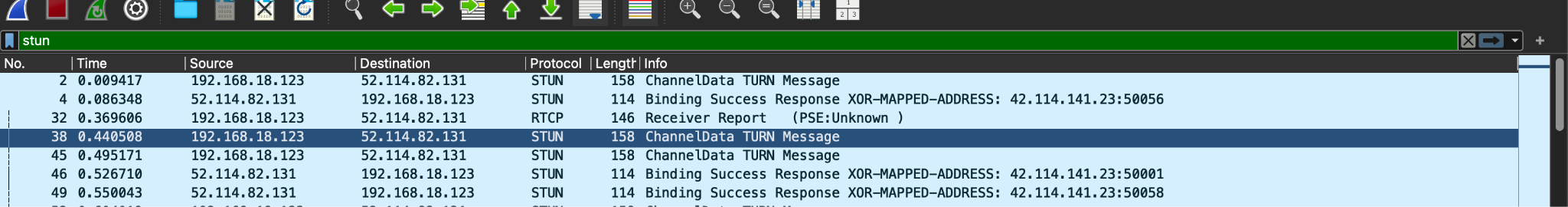
Cổng mặc định: Không cố định, thường đi kèm với RTP (cộng thêm 1 vào cổng RTP, ví dụ RTP 5004 thì RTCP 5005)



2. STUN (Session Traversal Utilities for NAT)

Chức năng: Cho phép thiết bị phía sau NAT tìm ra địa chỉ IP công khai và port của mình trên Internet. Thường dùng trong WebRTC, VoIP.

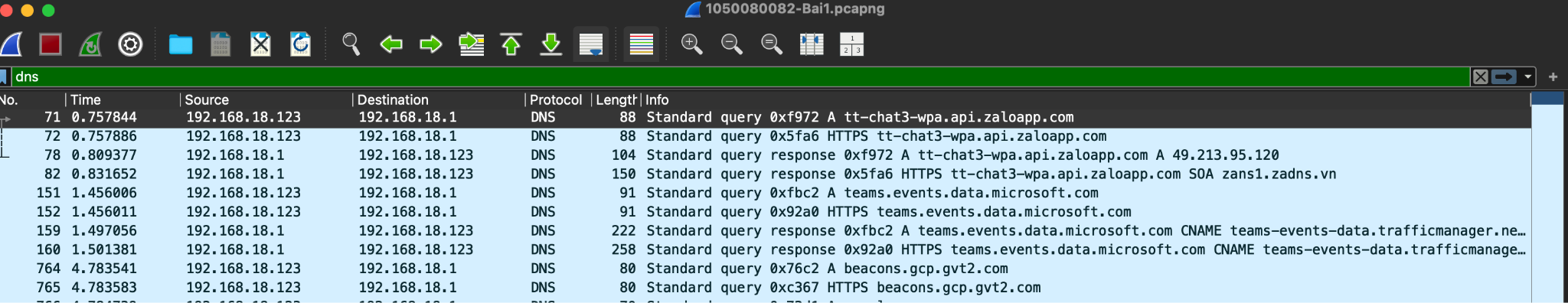
Cổng mặc định: 3478 (UDP/TCP)



3. DNS (Domain Name System)

Chức năng: Chuyển đổi tên miền (VD: google.com) thành địa chỉ IP (VD: 142.250.182.14) để trình duyệt có thể kết nối đúng máy chủ.

Cổng mặc định: 53 (UDP, đôi khi TCP)

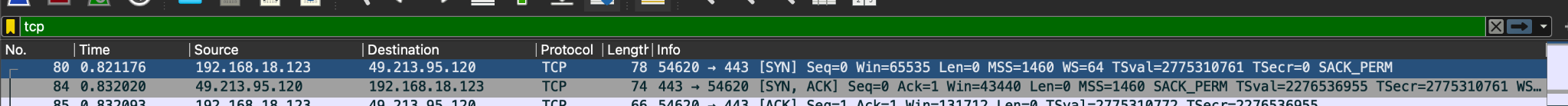


4. TCP (Transmission Control Protocol)

Chức năng: Giao thức truyền tải dữ liệu có kiểm soát, đảm bảo dữ liệu được gửi đầy đủ và theo đúng thứ tự.

Hoạt động cùng với nhiều giao thức ứng dụng khác như HTTP, SMTP.

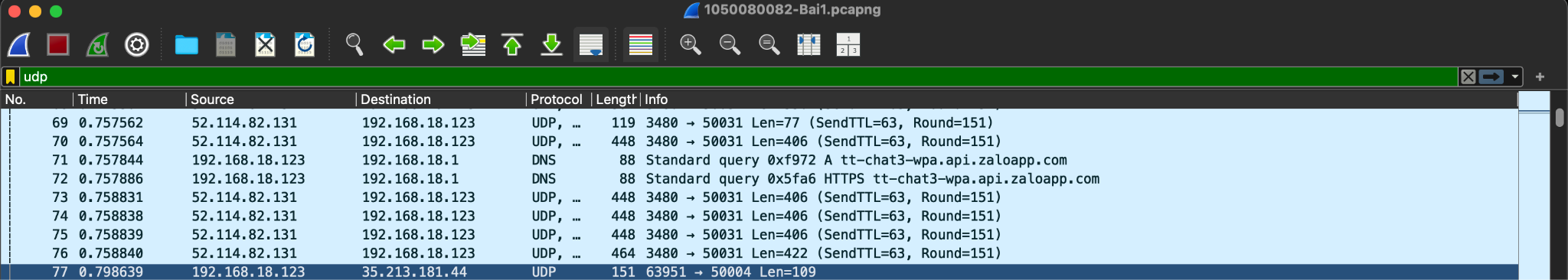
Cổng mặc định: Không có cổng cố định (tuỳ thuộc vào ứng dụng, VD: HTTP dùng 80, HTTPS dùng 443)



5. UDP (User Datagram Protocol)

Chức năng: Giao thức truyền tải dữ liệu nhanh hơn TCP nhưng không đảm bảo độ tin cậy, thường dùng trong VoIP, video streaming, game online.

Cổng mặc định: Không có cố định, tùy ứng dụng (VD: DNS sử dụng 53, STUN sử dụng 3478)



**3. Mất bao lâu từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi HTTP 200 OK đầu tiên được nhận đối với mỗi website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).**

* Không bắt được gói tin http

**4. Nội dung hiển thị trên trang** web gaia.cs.umass.edu

“Congratulations! You've downloaded the first Wireshark lab file!”

**có nằm trong các gói tin HTTP bắt được hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được.**

* Không có

**5. Địa chỉ IP của gaia.cs.umass.edu và website đã chọn ở bước 10 là gì? Địa chỉ IP của máy tính đang sử dụng là gì?**

* Không bắt được gói tin **gaia.cs.umass.edu**

**6. Qua ví dụ bắt gói tin trên và kết quả bắt gói tin từ Wireshark, hãy mô tả ngắn gọn diễn biến xảy ra khi bắt đầu truy cập vào một đường dẫn đến một trang web cho đến lúc xem được các nội dung trên trang web đó.**