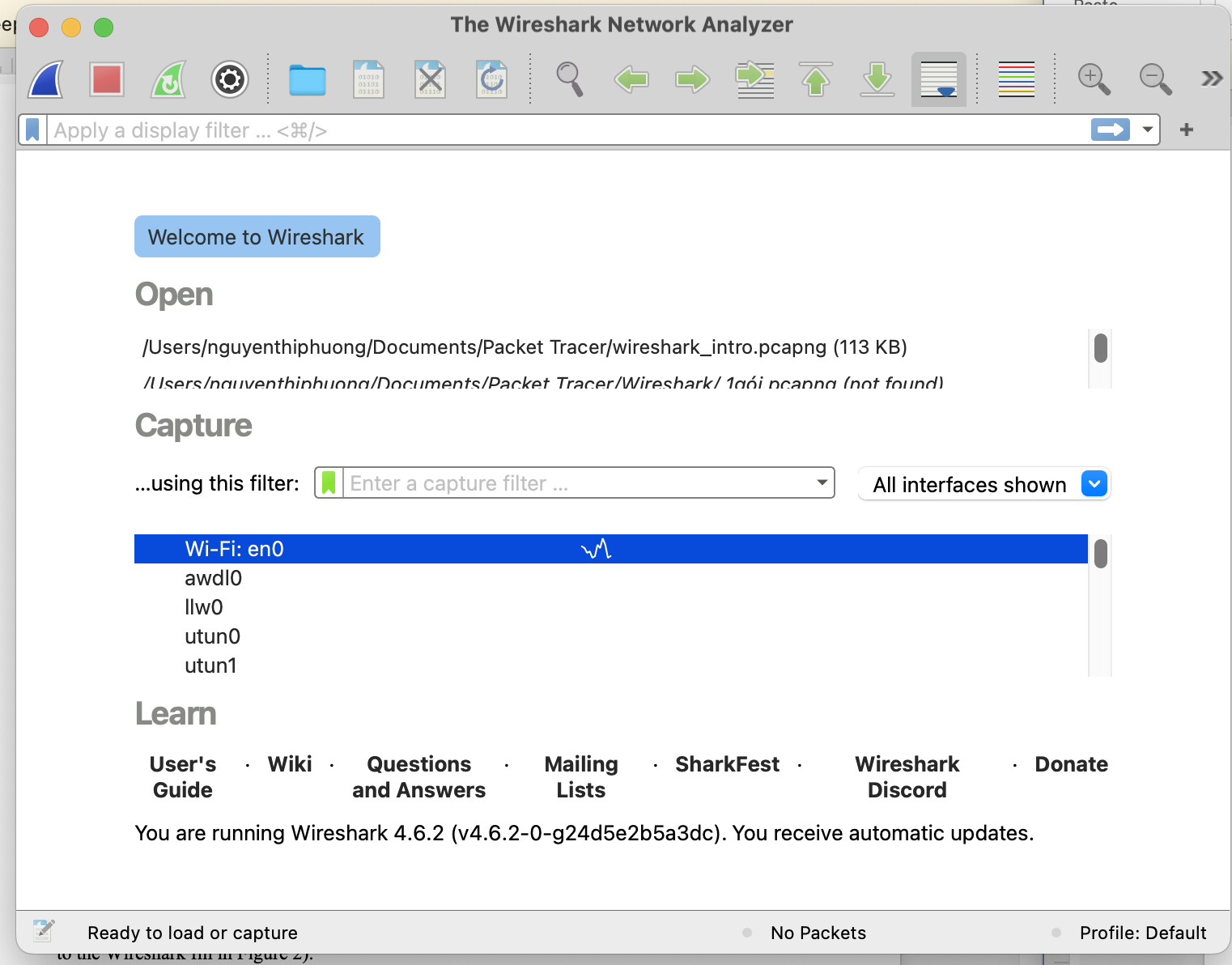
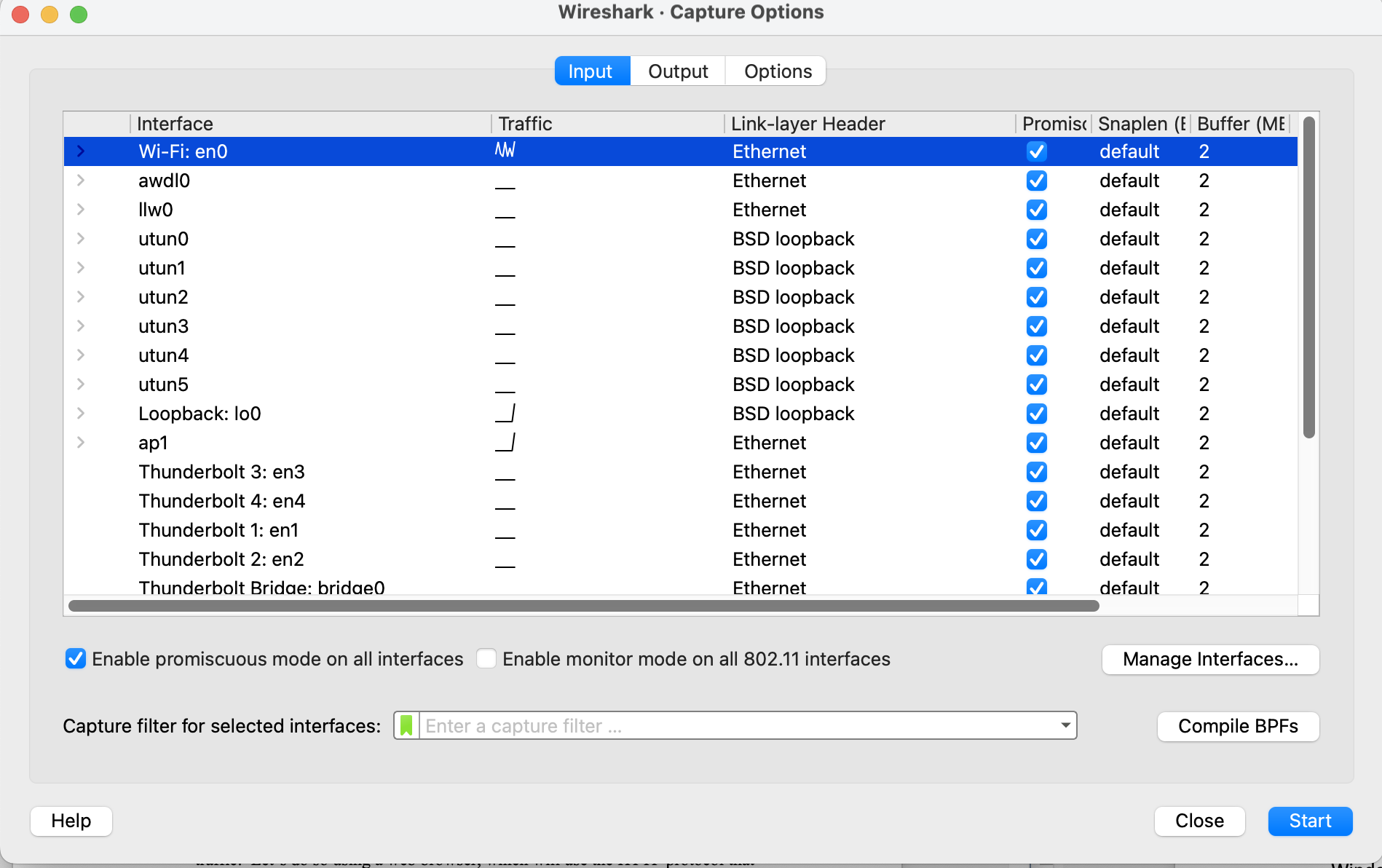
**Wireshark\_Intro\_v8.1**

Các bước của bài thực hành:

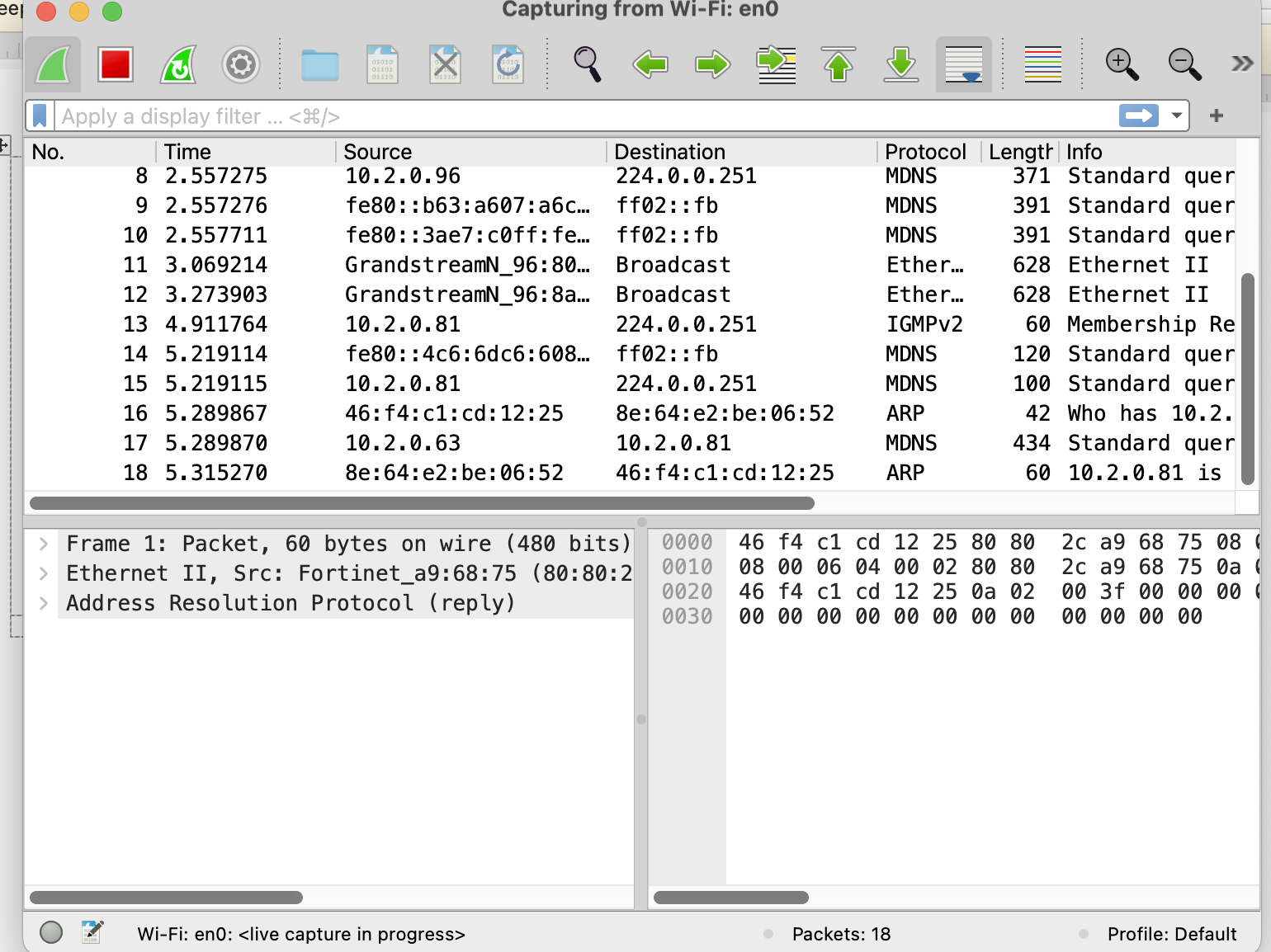
1. Khởi động trình duyệt Web của bạn, trình duyệt sẽ hiển thị trang chủ bạn đã chọn.
2. Khởi động phần mềm Wireshark. Wireshark chưa bắt đầu thu thập gói dữ liệu.



1. Để bắt đầu thu thập gói dữ liệu, chọn menu thả xuống Capture và chọn Interfaces. Thao tác này sẽ hiển thị cửa sổ “Wireshark: Capture Interfaces” (trên PC) hoặc bạn có thể chọn Options trên máy Mac. Sau đó bạn sẽ thấy danh sách các giao diện.

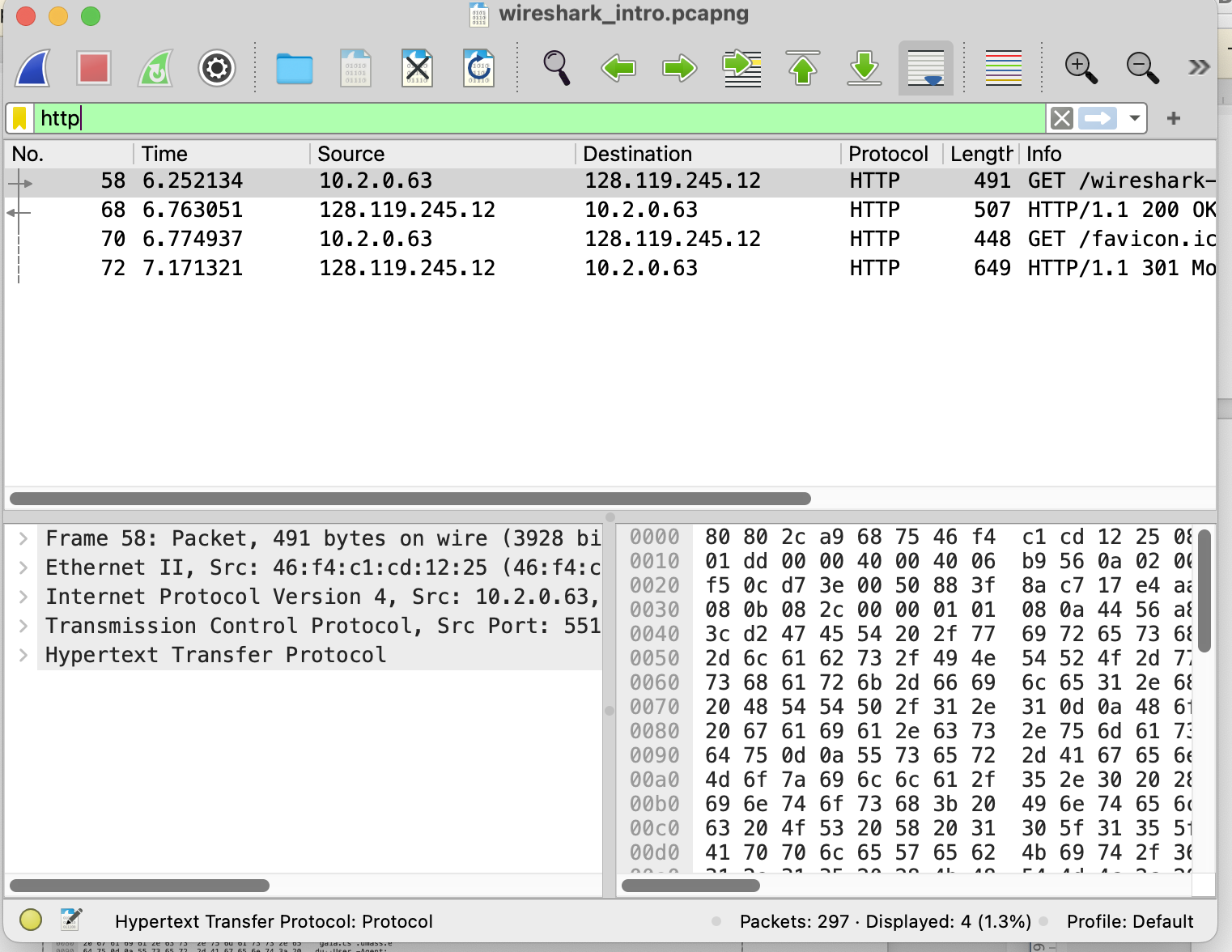


1. Bạn sẽ thấy danh sách các giao diện trên máy tính của mình cũng như số lượng gói tin đã được quan sát trên giao diện đó cho đến nay. Trên máy tính Windows, hãy nhấp vào Bắt đầu cho giao diện mà bạn muốn bắt đầu thu thập gói tin. Trên máy tính Windows, hãy chọn giao diện và nhấp vào Bắt đầu ở cuối cửa sổ. Quá trình thu thập gói tin sẽ bắt đầu - Wireshark hiện đang thu thập tất cả các gói tin được gửi/nhận từ/bởi máy tính của bạn!
2. Sau khi bạn bắt đầu thu thập gói tin, một cửa sổ sẽ hiện



Cửa sổ này hiển thị các gói tin đang được thu thập. Bằng cách chọn menu thả xuống Thu thập và chọn Dừng, hoặc bằng cách nhấp vào ô vuông màu đỏ Dừng, bạn có thể dừng quá trình thu thập gói tin. Nhưng đừng dừng quá trình thu thập gói tin ngay.

1. Trong khi Wireshark đang chạy, hãy nhập <URL:http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> và hiển thị trang đó trong trình duyệt của bạn. Để hiển thị trang này, trình duyệt của bạn sẽ liên hệ với máy chủ HTTP tại gaia.cs.umass.edu và trao đổi các thông điệp HTTP với máy chủ để tải xuống. Các khung Ethernet hoặc WiFi chứa các thông điệp HTTP này (cũng như tất cả các khung khác đi qua bộ chuyển đổi Ethernet hoặc WiFi của bạn) sẽ được Wireshark thu thập.
2. Sau khi trình duyệt của bạn đã hiển thị trang INTRO-wireshark-file1.html (đó chỉ là một dòng chúc mừng đơn giản), hãy dừng việc thu thập gói tin của Wireshark bằng cách chọn dừng trong cửa sổ thu thập của Wireshark. Bạn hiện đã có dữ liệu gói tin trực tiếp chứa tất cả các thông điệp giao thức được trao đổi giữa máy tính của bạn và các thực thể mạng khác! Các thông điệp HTTP được trao đổi với máy chủ web gaia.cs.umass.edu sẽ xuất hiện ở đâu đó trong danh sách các gói tin đã được thu thập.
3. Nhập "http" (không có dấu ngoặc kép và viết thường - tất cả tên giao thức đều viết thường trong Wireshark, và hãy nhớ nhấn phím Enter/Return) vào cửa sổ thông số bộ lọc hiển thị ở đầu cửa sổ chính của Wireshark. Sau đó chọn Áp dụng (ở bên phải chỗ bạn đã nhập “http”) hoặc chỉ cần nhấn Enter. Thao tác này sẽ chỉ hiển thị các thông báo HTTP trong cửa sổ liệt kê gói tin. Việc tập trung vào nội dung ở cấp độ thông báo, phân đoạn, gói dữ liệu và khung cụ thể cho phép chúng ta tập trung vào chính xác những gì chúng ta muốn xem (trong trường hợp này là các thông báo HTTP).



1. Tìm thông báo HTTP GET được gửi từ máy tính của bạn đến máy chủ HTTP gaia.cs.umass.edu. (Hãy tìm thông báo HTTP GET trong phần “danh sách các gói tin đã bắt được” của cửa sổ Wireshark hiển thị “GET” theo sau là URL gaia.cs.umass.edu mà bạn đã nhập. Khi bạn chọn thông báo HTTP GET, thông tin về khung Ethernet, gói dữ liệu IP, phân đoạn TCP và tiêu đề thông báo HTTP sẽ được hiển thị trong cửa sổ tiêu đề gói tin. Bằng cách nhấp vào ‘+’ và ‘-’ và các mũi tên chỉ sang phải và chỉ xuống ở phía bên trái của cửa sổ chi tiết gói tin, hãy giảm thiểu lượng thông tin về Khung, Ethernet, Giao thức Internet và Giao thức Điều khiển Truyền tải được hiển thị.
2. Thoát Wireshark

Câu hỏi

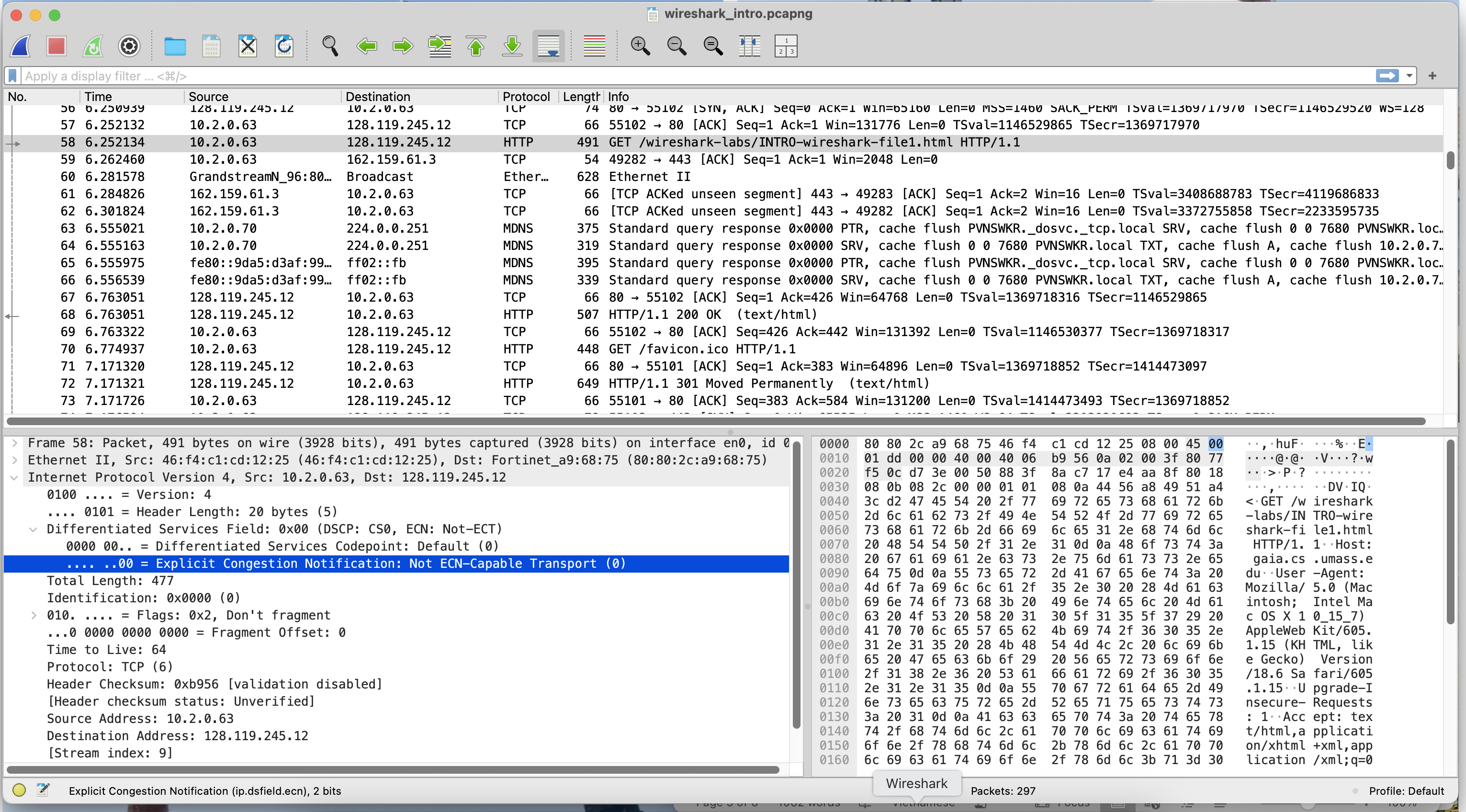
1. Giao thức nào sau đây được hiển thị (tức là được liệt kê trong cột “giao thức” của Wireshark) trong tệp theo dõi của bạn: TCP, QUIC, HTTP, DNS, UDP, TLSv1.2?

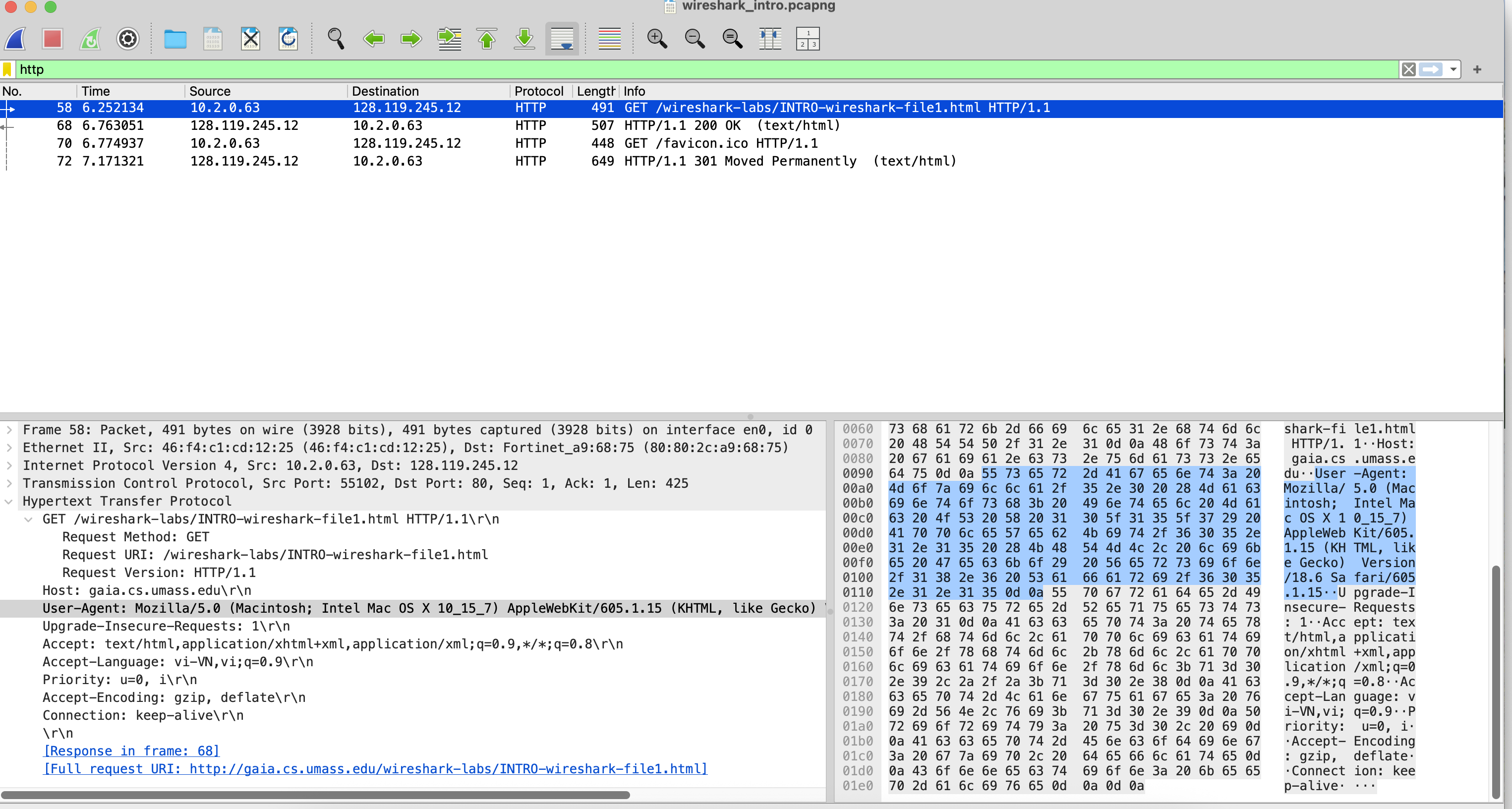
***🡺 Các giao thức hiển thị trong file theo dõi là: TCP, QUIC, HTTP, UDP và TLSv1.2. Giao thức DNS không xuất hiện ( mà xuất hiện giao thức MDNS)***

1. Mất bao lâu kể từ khi thông báo HTTP GET được gửi cho đến khi nhận được phản hồi HTTP OK? (Theo mặc định, giá trị của cột Thời gian trong cửa sổ liệt kê gói tin là khoảng thời gian, tính bằng giây, kể từ khi bắt đầu theo dõi Wireshark. (Nếu bạn muốn hiển thị trường Thời gian ở định dạng giờ trong ngày, hãy chọn menu thả xuống Chế độ xem Wireshark, sau đó chọn Định dạng hiển thị thời gian, sau đó chọn Giờ trong ngày.)?

***🡺 Mất khoảng 0.51 giây kể từ khi thông báo HTTP GET được gửi đi cho đến khi nhận phản hồi HTTP 200 OK (6.763051 – 6.252134 = 0.510917)***

1. Địa chỉ Internet của gaia.cs.umass.edu (còn được gọi là www-net.cs.umass.edu) là gì? Địa chỉ Internet của máy tính của bạn hoặc (nếu bạn đang sử dụng tệp theo dõi) của máy tính đã gửi thông báo HTTP GET là gì?

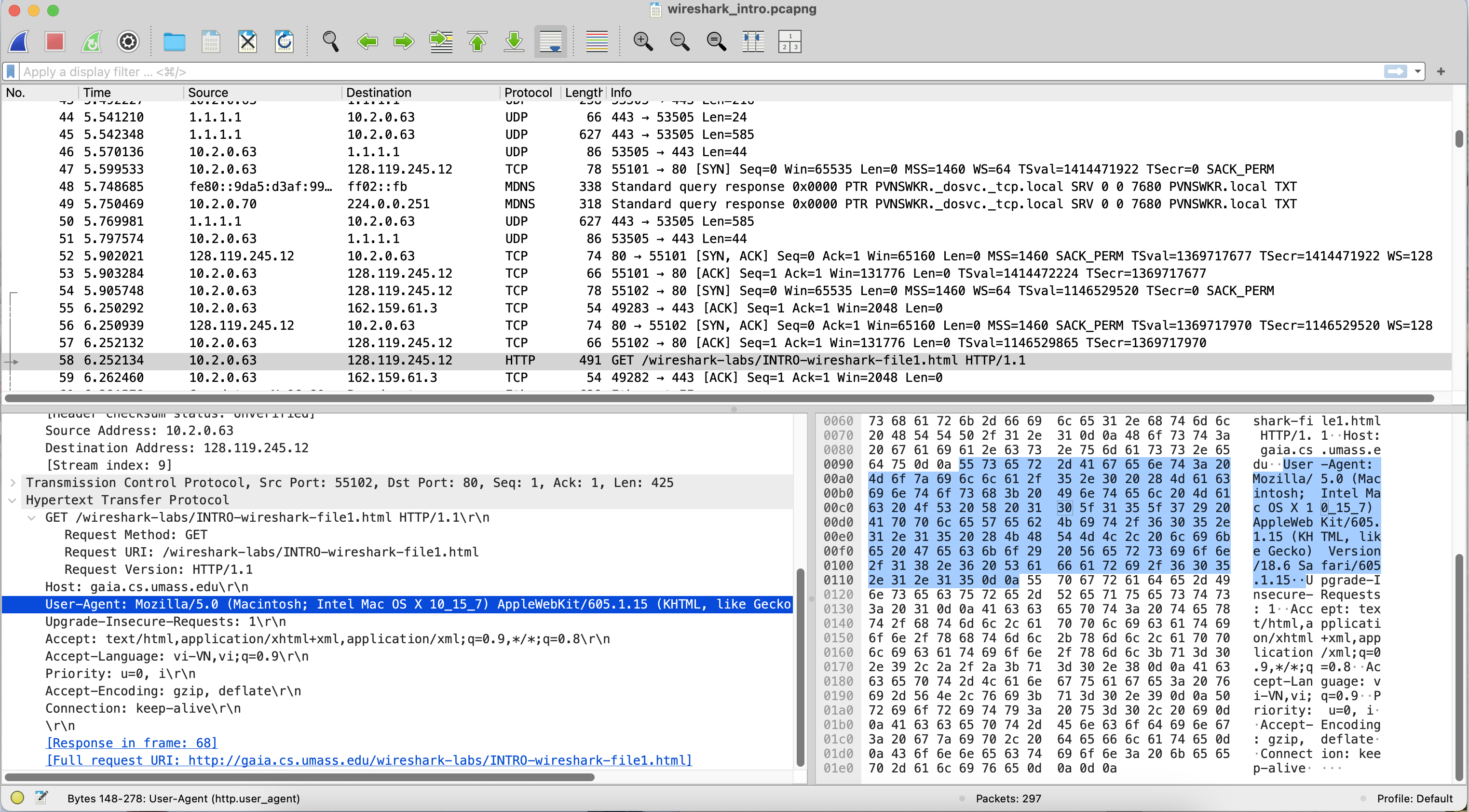




***🡺 Địa chỉ Internet của gaia.cs.umass.edu (còn được gọi là www-net.cs.umass.edu) là: 128.119.245.12***

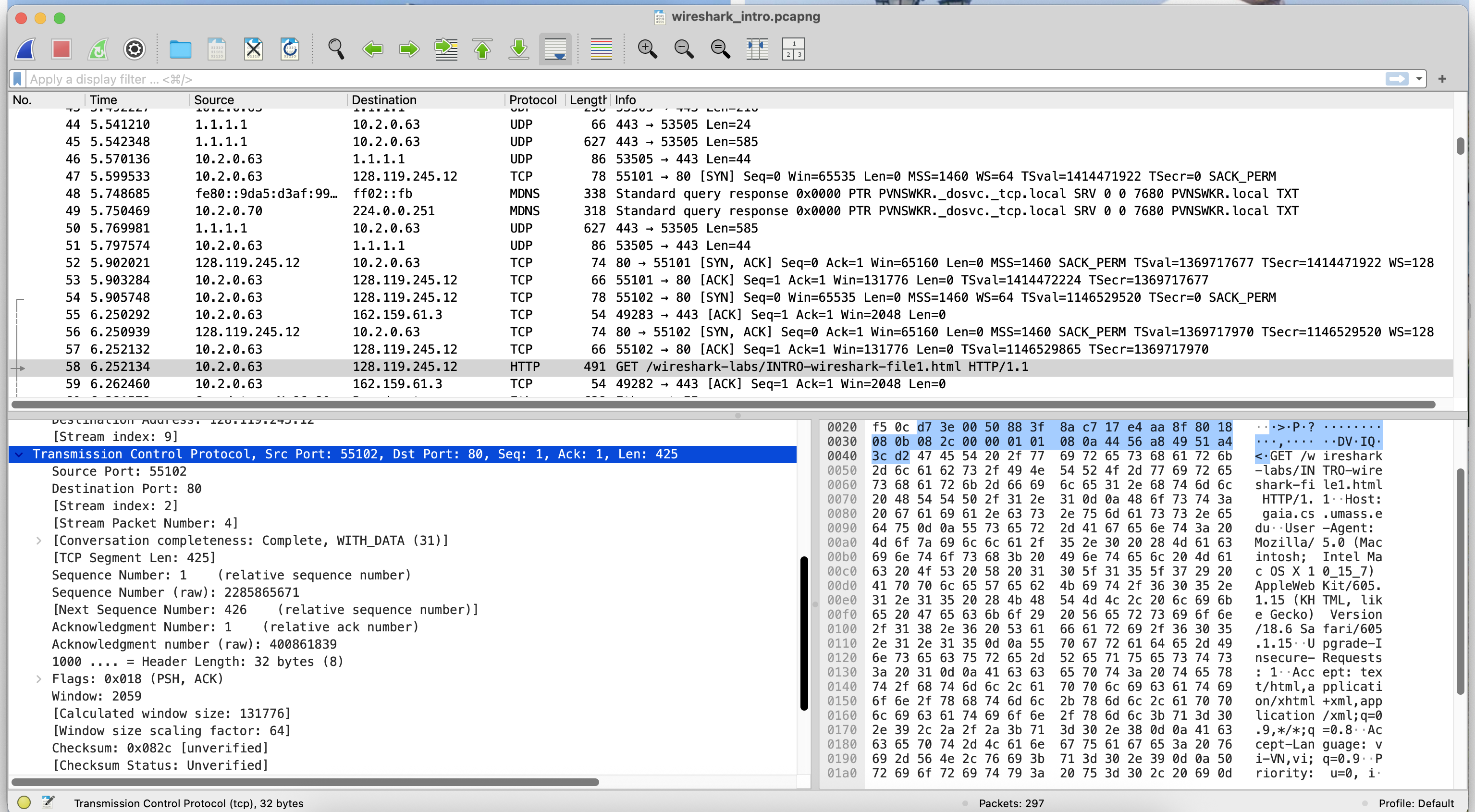
***🡺 Địa chỉ Internet của máy tính của bạn hoặc (nếu bạn đang sử dụng tệp theo dõi) của máy tính đã gửi thông báo HTTP GET là: 10.2.0.63***

1. Mở rộng thông tin về thông báo HTTP trong cửa sổ “Chi tiết gói tin đã chọn” của Wireshark (xem Hình 3 ở trên) để bạn có thể thấy các trường trong thông báo yêu cầu HTTP GET. Loại trình duyệt web nào đã gửi yêu cầu HTTP?



***🡺 Loại trình duyệt wed đã gửi yêu cầu HTTP GET là: Safari***

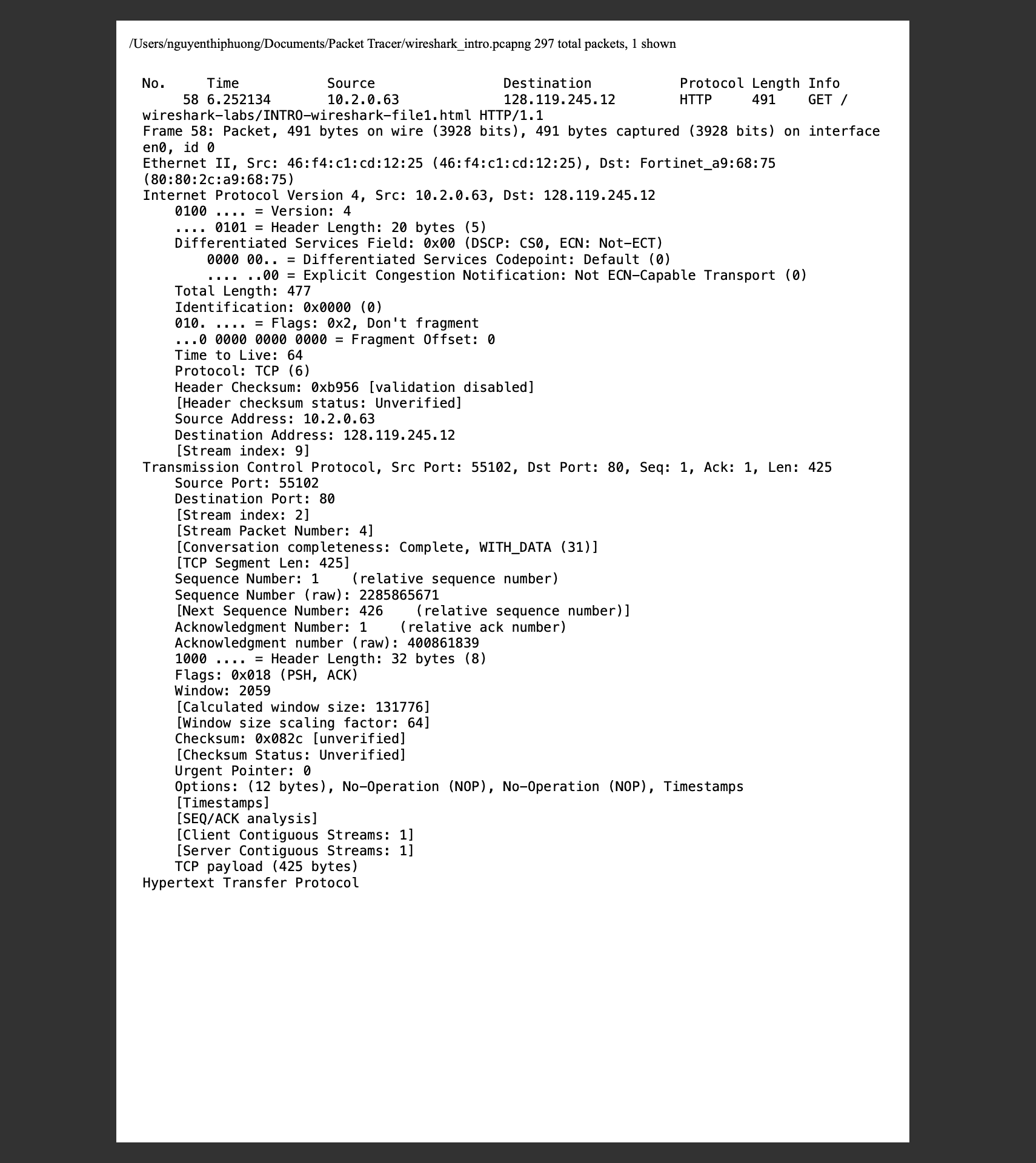
5. Mở rộng thông tin về Giao thức Điều khiển Truyền tải (TCP) cho gói tin này trong cửa sổ “Chi tiết gói tin đã chọn” của Wireshark (xem Hình 3 trong bài hướng dẫn thực hành) để bạn có thể thấy các trường trong phân đoạn TCP mang thông điệp HTTP. Số cổng đích (số sau “Cổng đích:” cho phân đoạn TCP chứa yêu cầu HTTP) mà yêu cầu HTTP này đang được gửi đến là gì?



***🡺 Số cổng đích (Destination Port) mà HTTP đang được gửi đến là: 80***

1. In hai thông báo HTTP (GET và OK) được đề cập trong câu hỏi 2 ở trên. Để làm vậy, chọn Print từ menu lệnh File của Wireshark, chọn các nút tròn “Selected Packet Only” và “Print as displayed”, rồi nhấn OK.

* HTTP GET



* HTTP OK

