

Lab

1

BÁO CÁO BÀI THỰC HÀNH SỐ 1
Làm quen với Wireshark
Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Sinh viên thực hiện	Dương Thuận Trí (22521517)
Thời gian thực hiện	27/09/2023- 04/10/2023
Tự chấm điểm	10/10

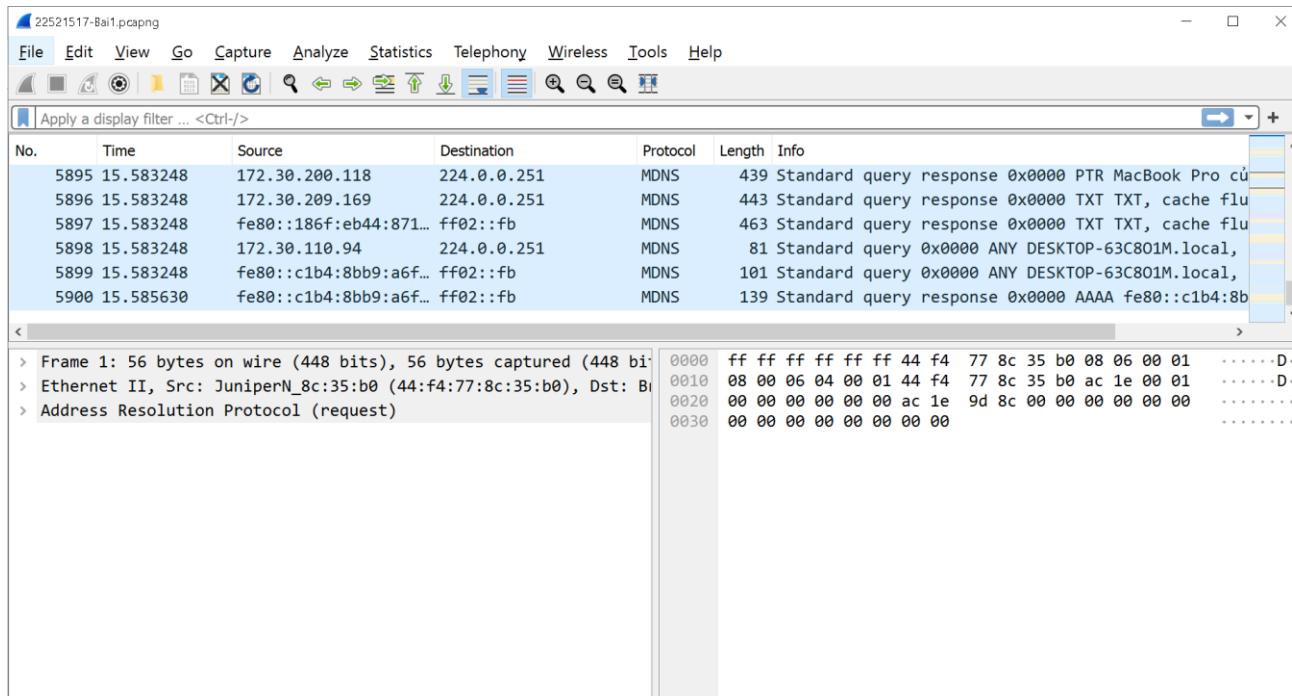
TRẢ LỜI CÁC CÂU HỎI

Gợi ý: Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn.

Câu 1. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

Trả lời: Tổng thời gian bắt gói tin là 15.58560 giây, tổng số gói tin bắt được là 5900

Để xem tổng thời gian bắt gói tin và tổng số gói tin bắt được, ta kéo xuống tìm đến gói tin cuối cùng (trước khi dừng bắt gói tin) và xem số thứ tự của nó (No.) để biết tổng số gói tin, thời gian lúc bắt được nó (Time) để biết tổng thời gian bắt gói tin.

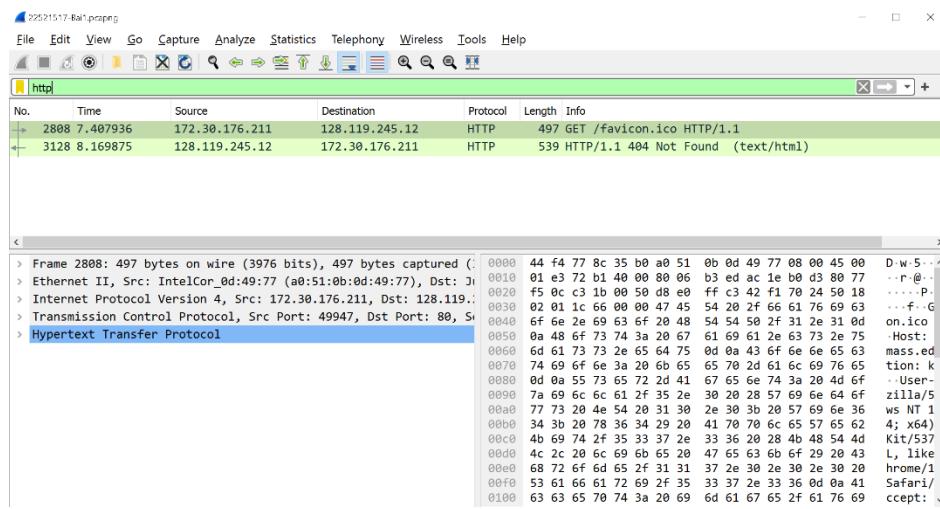


Câu 2: Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol). Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

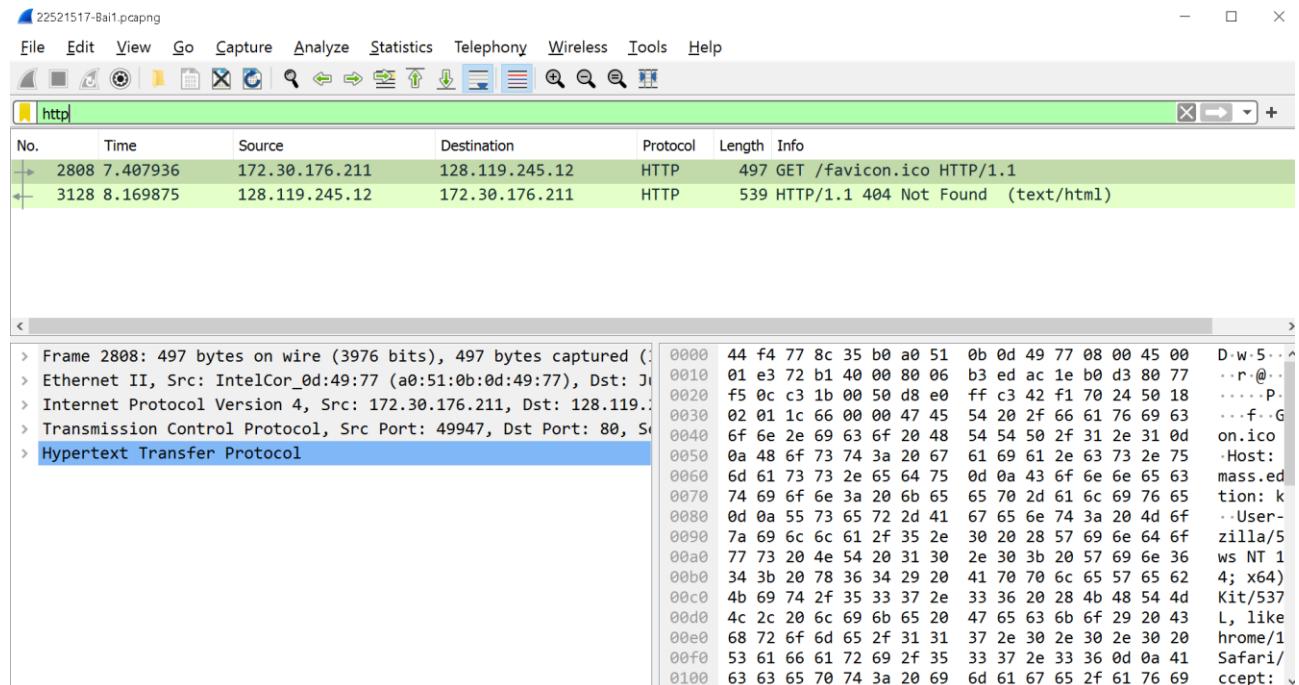
Trả lời: Các giao thức khác nhau xuất hiện trong cột giao thức (Protocol): Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), Address Resolution Protocol (ARP).

Lab 1: Làm quen với Wireshark

Transmission Control Protocol (TCP): là giao thức cốt lõi của Internet Protocol Suite. TCP bắt nguồn từ việc thực thi mạng, bổ sung cho Internet Protocol. Do đó, Internet Protocol Suite thường được gọi là TCP/IP. TCP cung cấp một phương thức phân phối đáng tin cậy một luồng octet (khối dữ liệu có kích thước 8 bit) qua mạng IP. Đặc điểm chính của TCP là khả năng đưa ra lệnh và kiểm tra lỗi. Tất cả các ứng dụng Internet lớn như World Wide Web, email và truyền file đều dựa vào TCP.

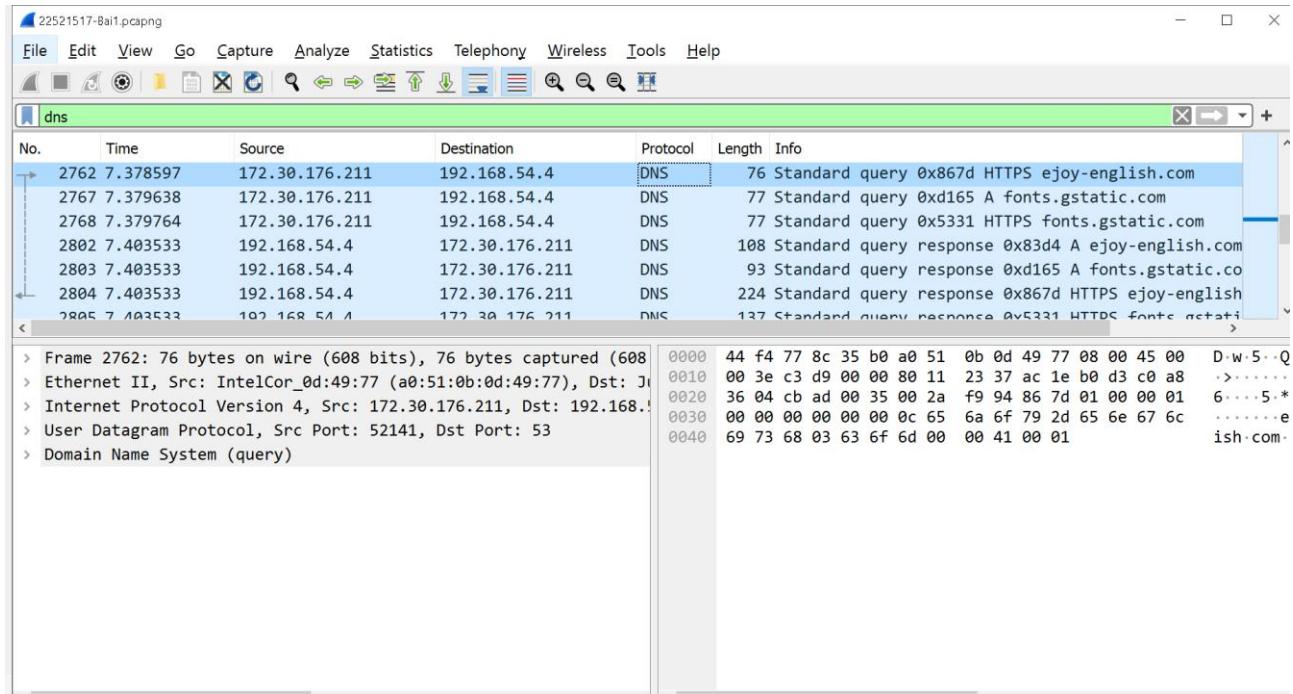


Hypertext Transfer Protocol (HTTP): nền tảng giao tiếp dữ liệu cho World Wide Web. Siêu văn bản (hypertext) là văn bản có cấu trúc sử dụng các siêu liên kết giữa các node chứa văn bản. HTTP là giao thức ứng dụng cho hệ thống thông tin hypermedia (siêu phương tiện) phân tán và kết hợp.

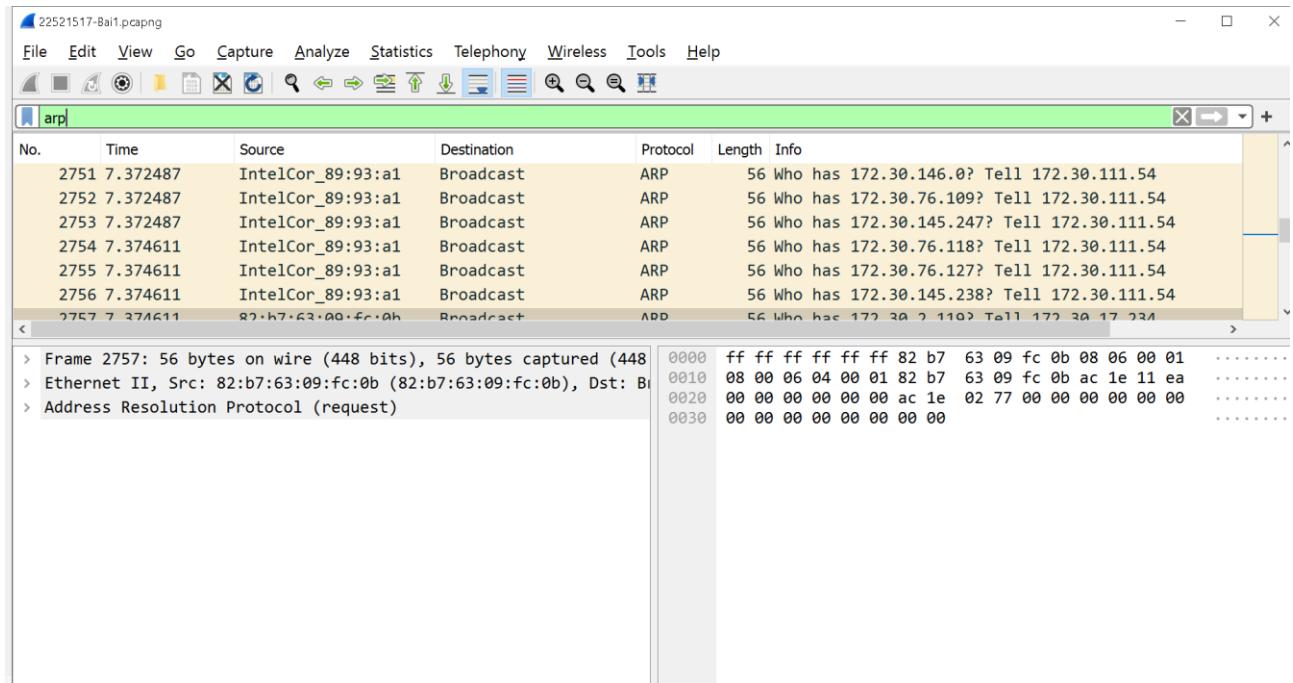


Lab 1: Làm quen với Wireshark

Domain Name System (DNS): là một hệ thống phân giải tên miền. Hệ thống này là một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên internet. Nhờ giao thức này nên có thể chuyển đổi tên miền thành địa chỉ IP. Cổng mặc định của DNS là 53.



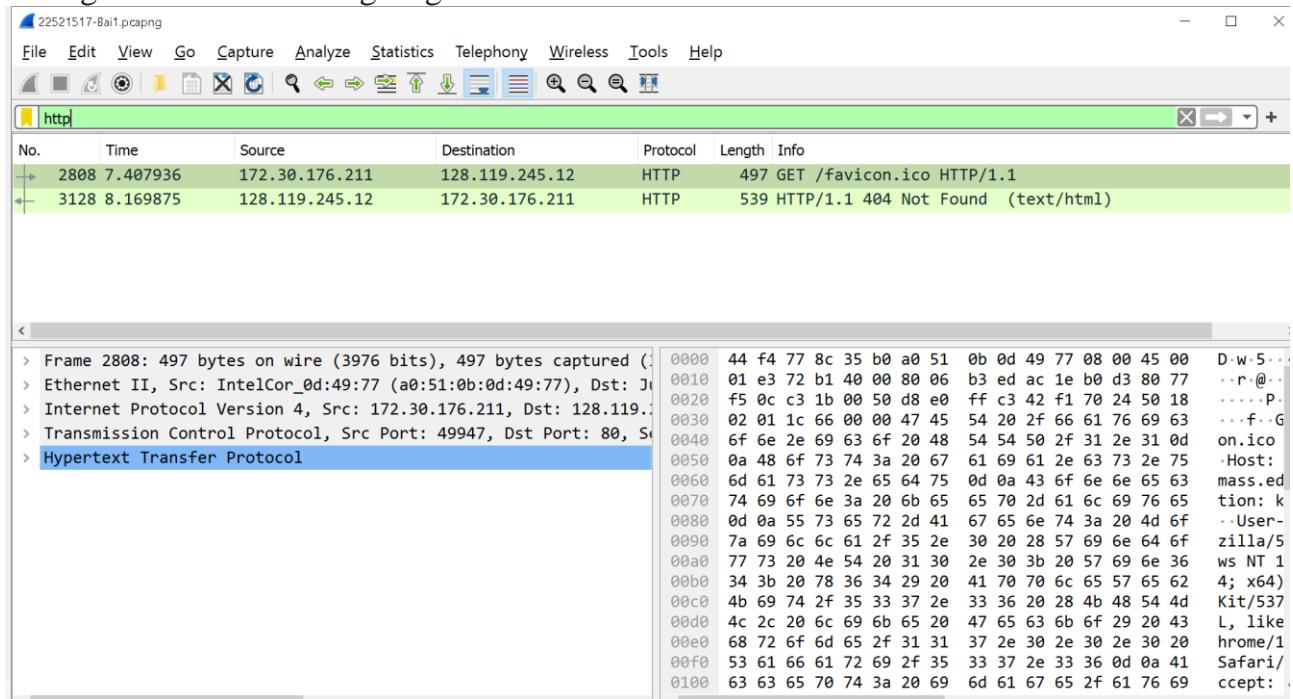
Address Resolution Protocol (ARP): là giao thức mạng được dùng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn. Nó được sử dụng khi một thiết bị giao tiếp với các thiết bị khác dựa trên nền tảng local network. Ví dụ như trên mạng Ethernet mà hệ thống yêu cầu địa chỉ vật lý trước khi thực hiện gửi packets.



Lab 1: Làm quen với Wireshark

Câu 3: Có bao nhiêu gói tin HTTP? Tỉ lệ % số gói tin HTTP/Tổng số gói tin?

Trả lời: Có 2 gói tin HTTP. Tỉ lệ % số gói tin HTTP/Tổng số gói tin: 0,0003389831%
Có 2 gói tin HTTP và tổng số gói tin là 5900



Câu 4: Có bao nhiêu gói tin HTTP GET?

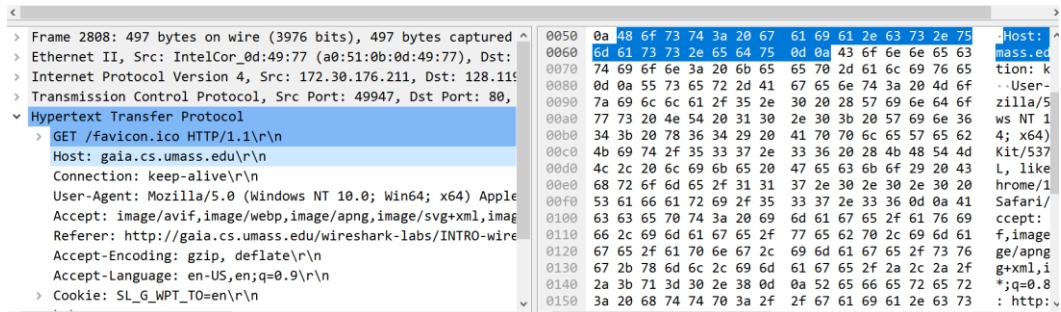
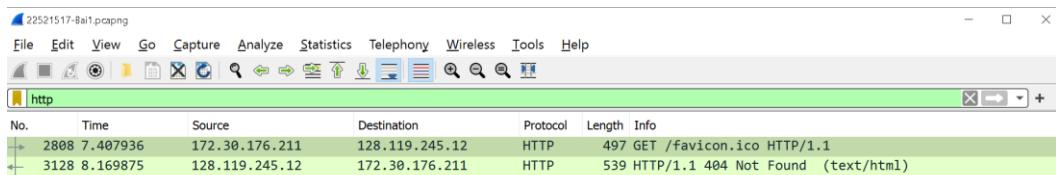
Trả lời: Có 1 gói tin HTTP GET

+	2808 7.407936	172.30.176.211	128.119.245.12	HTTP	497 GET /favicon.ico HTTP/1.1
---	---------------	----------------	----------------	------	-------------------------------

Câu 5: Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server

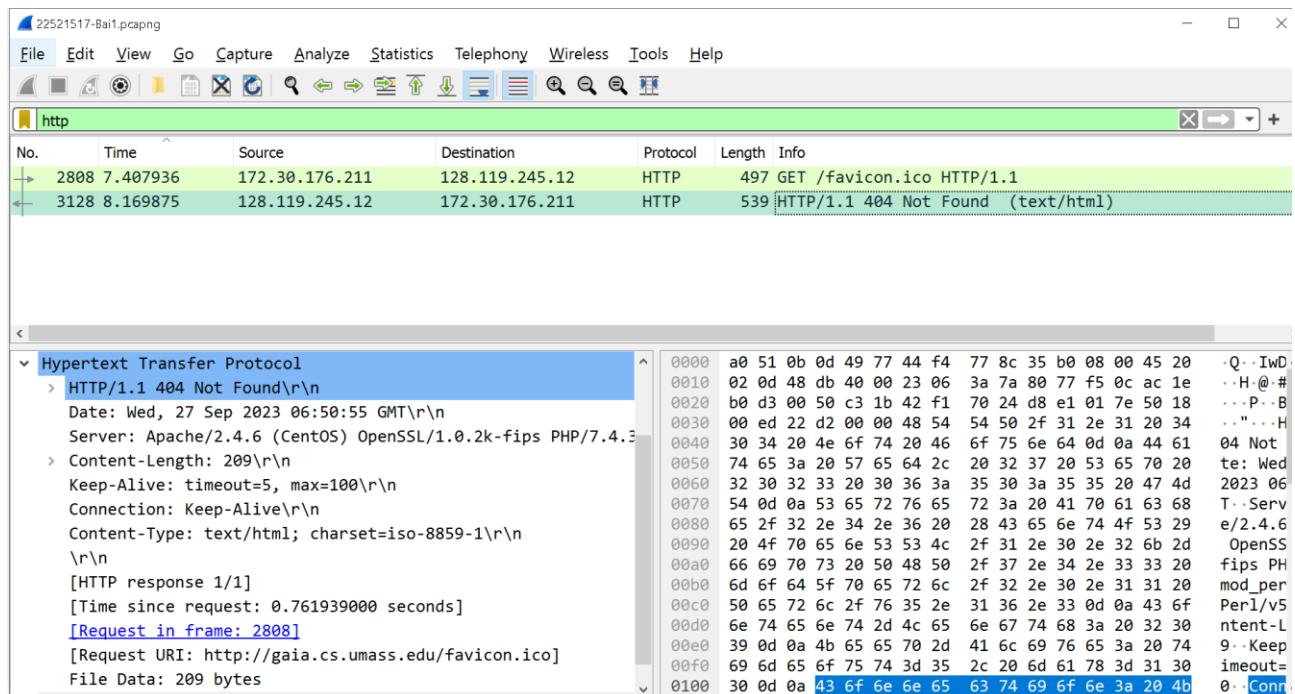
Trả lời: Gói HTTP Get đầu tiên có số thứ tự là 2808

Lab 1: Làm quen với Wireshark



Câu 6: Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?

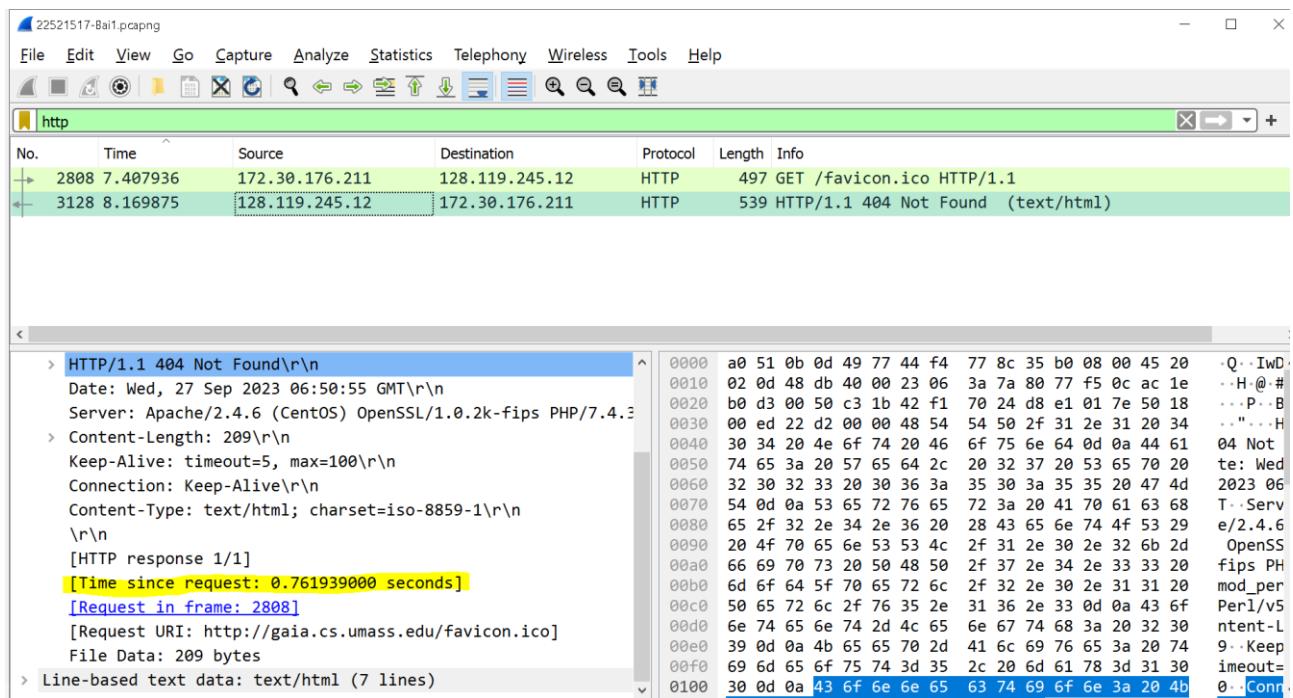
Trả lời: Gói tin phản hồi cho gói HTTP GET có số thứ tự là 3128 (vì gói tin này có Request in frame là 2808 (chính là số thứ tự của gói tin GET))



Câu 7: Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)?

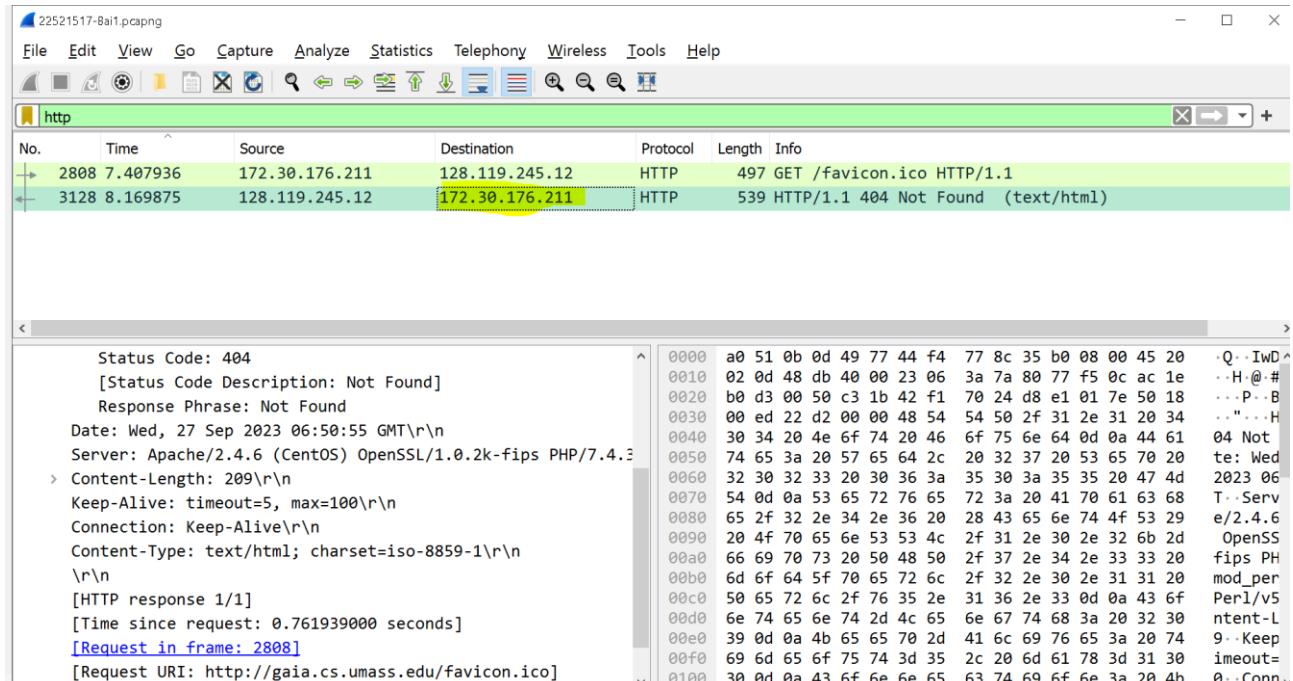
Trả lời: Mất 0.761939000 giây từ lúc gửi gói tin HTTP GET đến khi nhận được gói tin phản hồi

Lab 1: Làm quen với Wireshark



Câu 8: Dự đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì? Tại sao?

Trả lời: Dự đoán địa chỉ IP của gaia.cs.umass.edu là: 128.119.245.12 (địa chỉ request). Địa chỉ IP của máy tính đang sử dụng là 172.30.176.211 vì địa chỉ của gói tin phản hồi cũng chính là địa chỉ của máy tính đang sử dụng.

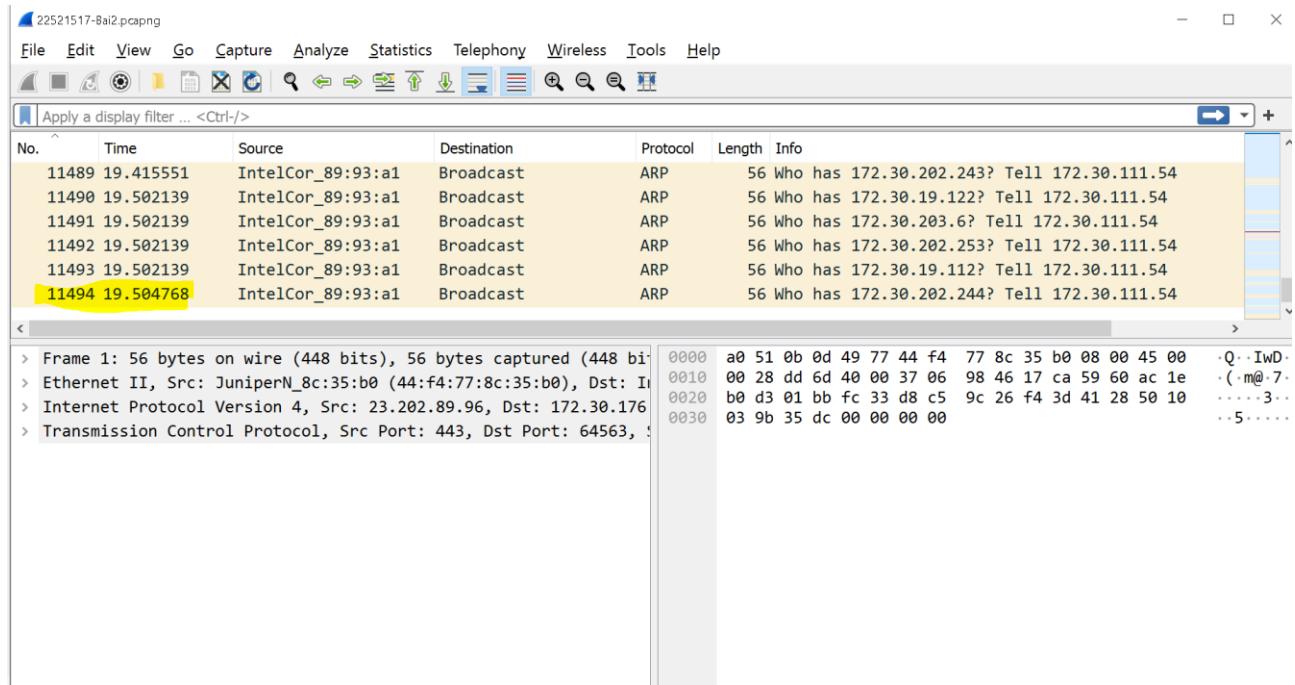


Lab 1: Làm quen với Wireshark

Câu 9: Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?

Trả lời: Tổng thời gian bắt gói tin là 19.504768 giây và tổng số gói tin bắt được là 11494 gói

Xem số thứ tự và thời gian bắt của gói tin cuối cùng để xác định.



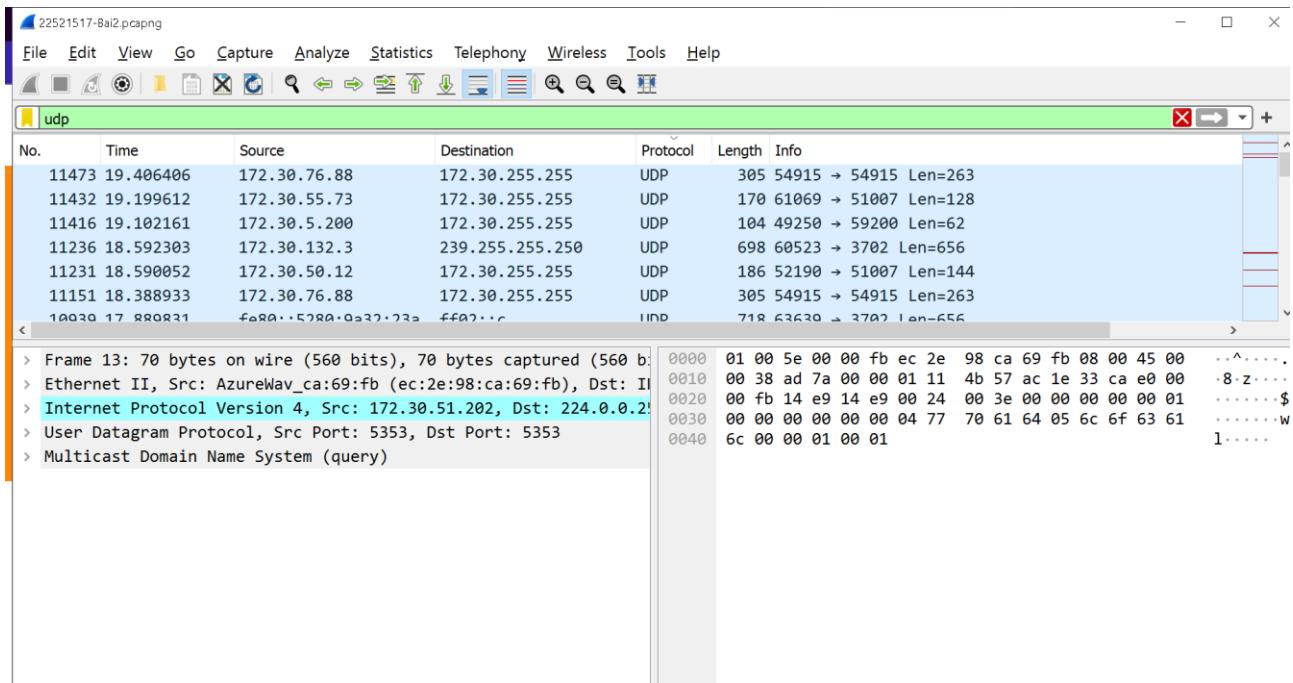
Câu 10: Liệt kê ít nhất 3 giao thức khác nhau xuất hiện trong cột giao thức (Protocol).

Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

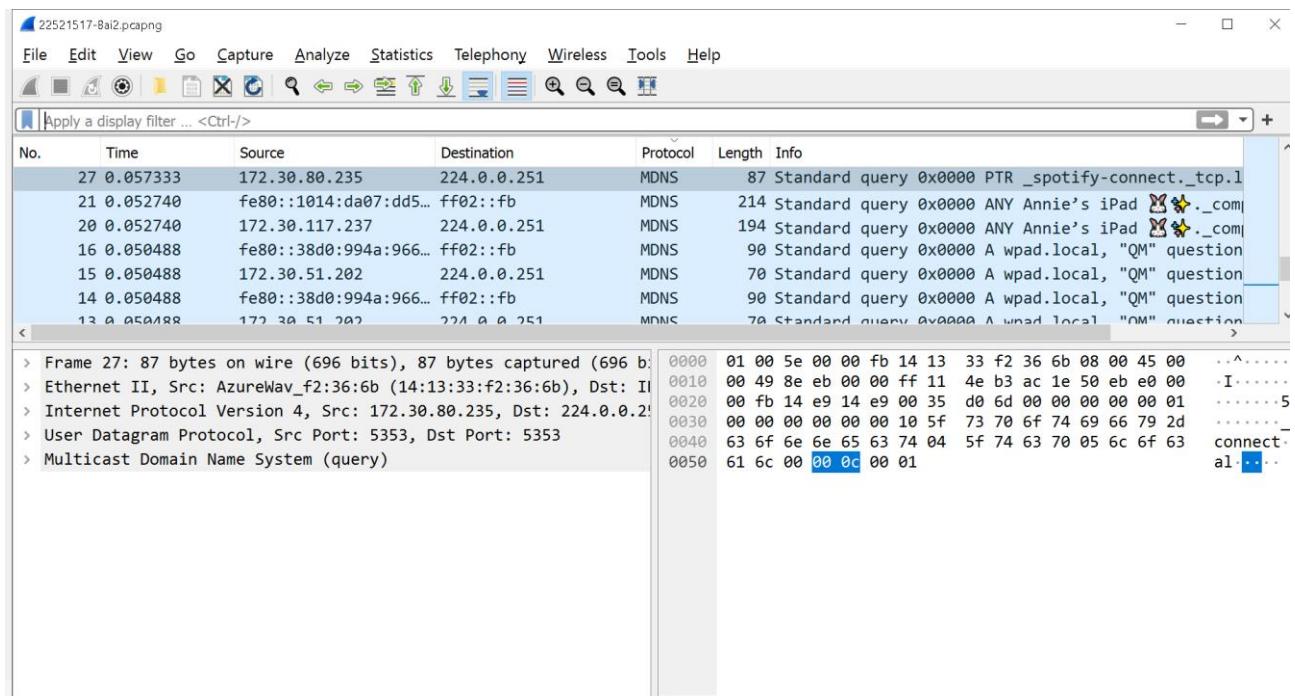
Trả lời:

- User Datagram Protocol (UDP): là một trong những giao thức cốt lõi của giao thức TCP/IP. Dùng UDP, chương trình trên mạng máy tính có thể gửi những dữ liệu ngắn được gọi là datagram tới máy khác. UDP không cung cấp sự tin cậy và thứ tự truyền nhận mà TCP làm; các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. Tuy nhiên UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian. Do bản chất không trạng thái của nó nên nó hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu.

Lab 1: Làm quen với Wireshark

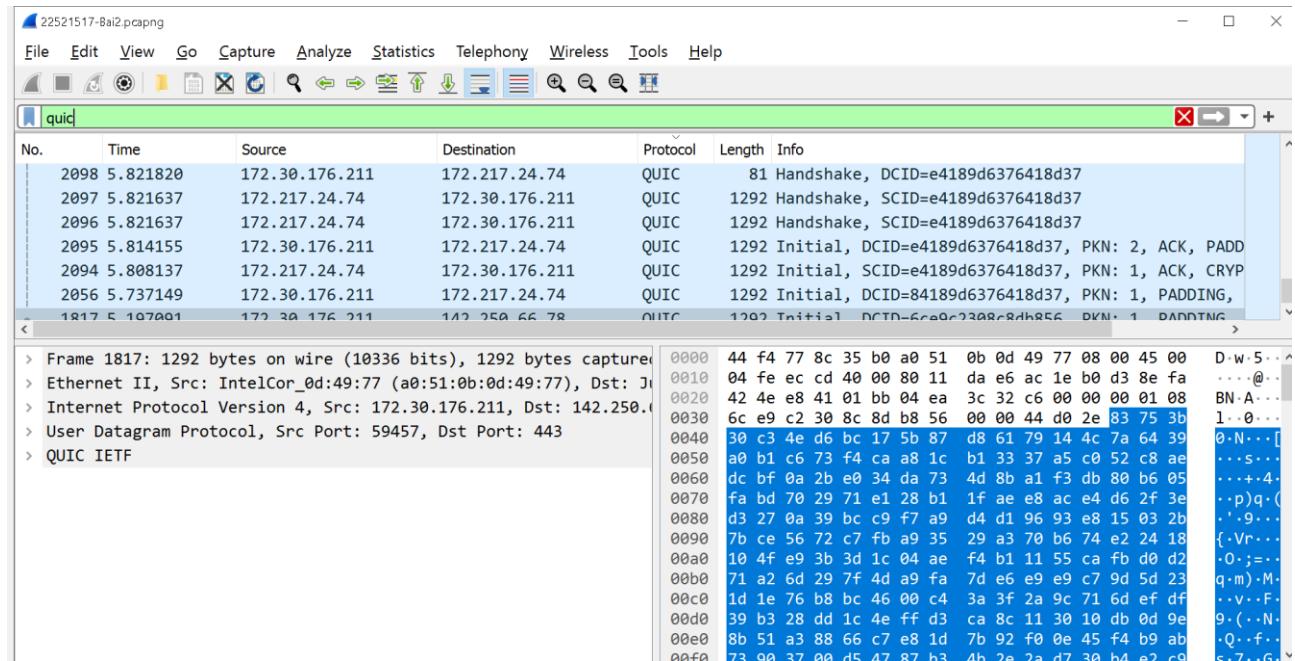


- Multicast DNS (mDNS): là một dịch vụ cơ bản cho một số ứng dụng IoT có thể thực hiện các nhiệm vụ của máy chủ DNS unicast [15]. Một dịch vụ mDNS là linh hoạt do thực tế không gian tên DNS sử dụng tại địa phương không cần thêm chi phí hoặc cấu hình. mDNS là sự lựa chọn thích hợp cho các thiết bị nhúng dựa trên Internet do không cần phải cấu hình lại, có thể chạy không cần cơ sở hạ tầng, có thể tiếp tục làm việc nếu cơ sở hạ tầng thất bại. mDNS truy vấn bằng cách gửi một tin nhắn IP multicast cho tất cả các nút trong miền địa phương. Bằng cách này, các khách hàng yêu cầu thiết bị được đặt để trả lời lại. Khi các máy tính mục tiêu nhận được tên của nó, sẽ multicast một tin nhắn phản ứng, trong đó có địa chỉ IP của nó. Tất cả các thiết bị trong mạng có được các tin nhắn phản ứng cập nhật tại bộ nhớ đệm địa phương của nó bằng tên và địa chỉ IP.



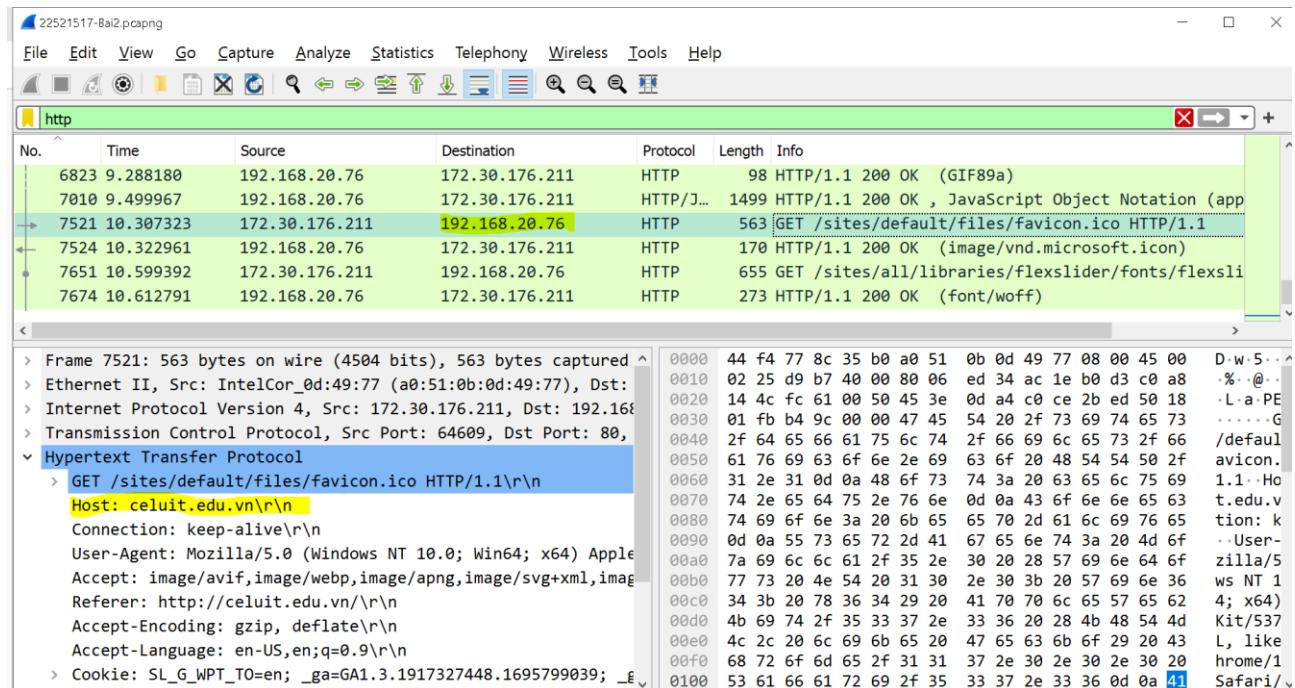
Lab 1: Làm quen với Wireshark

- Quick Connections UDP Internet (QUIC -Giao thức kết nối Internet nhanh UDP) , đây là một giao thức truyền tải do Google phát triển nhằm thay thế cho giao thức TCP. QUIC chạy một dòng giao thức ghép kênh trên UDP thay vì TCP.



Câu 11: Tìm cách để xác định địa chỉ IP của trang web đã chọn ở Bước 8. Địa chỉ IP trang web đã chọn là gì ?

Trả lời: Địa chỉ của trang web celuit.edu.vn là 192.168.20.76



Câu 12: Số lượng gói tin và khối lượng dữ liệu được gửi (trao đổi) giữa Địa chỉ trang web ở trên (Câu 11) và máy tính đang sử dụng ?

Trả lời: Số lượng gói tin là 119 gói, khối lượng dữ liệu 74kB.

