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	Đoàn Phương Nam (22520908)
Thời gian thực hiện	27/09/2023
Tự chấm điểm	10/10

TRẢ LỜI CÁC CÂU HỎI

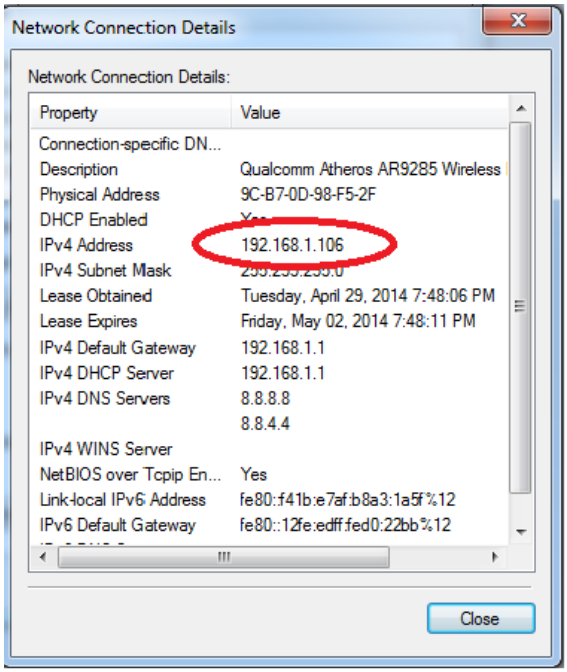
Gợi ý: *Trả lời câu hỏi đúng, đầy đủ, cần giải thích lý do tại sao có được đáp án, có các hình ảnh, bằng chứng để chứng minh tính đúng đắn*.

Ví dụ:

Câu 1. Địa chỉ IP máy tính của bạn là gì?

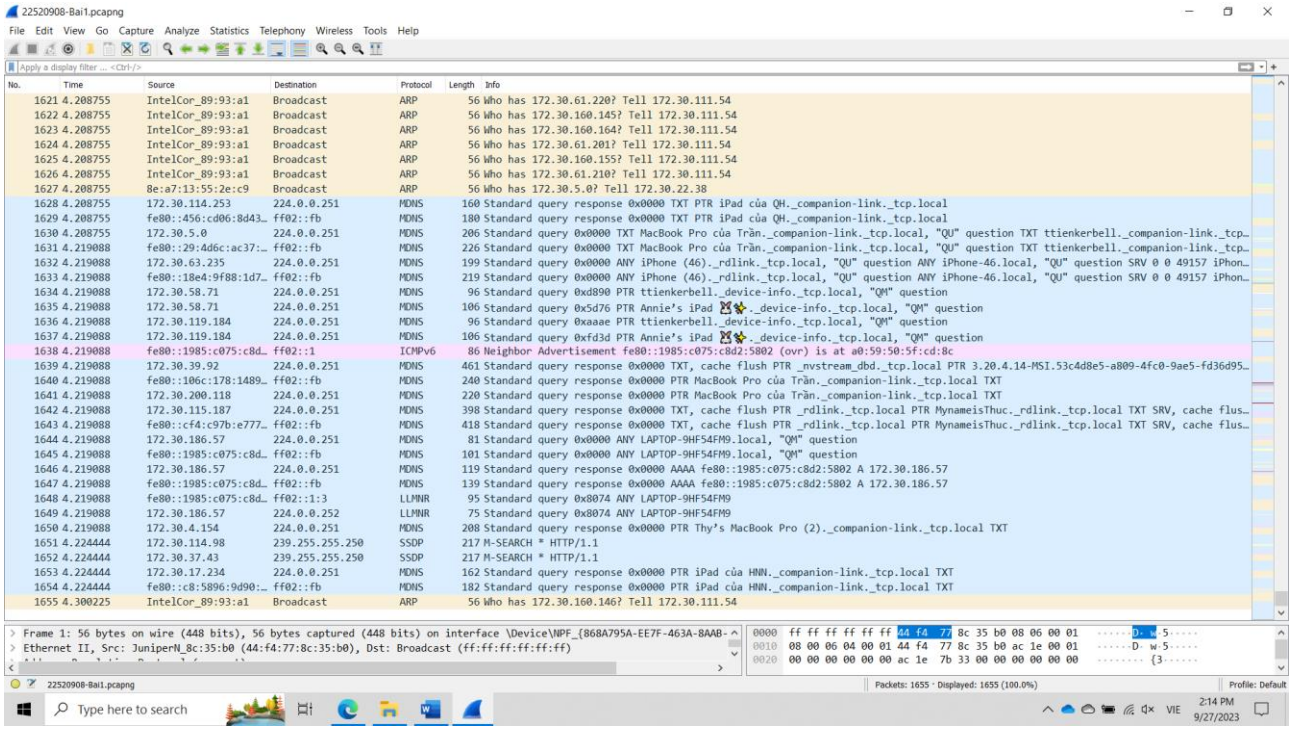
Trả lời: *192.168.1.106*

Để xem địa chỉ IP của máy tính trên Windows, mở **Control Panel** và chọn **View network status and tasks.** Chọn mạng tương ứng đang sử dụng để kết nối Internet, chọn **Details** trong cửa sổ trạng thái. Xem địa chỉ IP trong Ipv4 Address



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

Trả lời: tổng số gói tin bắt được: 1655 mất 4.30025s



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:

LLMNR:

1. Giải quyết tên máy tính: cho phép các thiết bị trong cùng một mạng cục bộ gửi các yêu cầu giải quyết tên máy tính (name resolution requests) cho các máy tính khác trong mạng mà họ muốn kết nối
2. Hoạt động trong mạng cục bộ: được sử dụng chủ yếu trong các mạng cục bộ, nơi máy tính và thiết bị kết nối trực tiếp vào mạng mà không có sự tham gia của máy chủ DNS trung gian.
3. Sử dụng giao thức đa phương tiện: sử dụng giao thức đa phương tiện để gửi yêu cầu giải quyết tên và nhận phản hồi từ các thiết bị khác trong mạng.
4. Hỗ trợ trình động tên máy tính: cho phép các thiết bị tự động cập nhật thông tin giải quyết tên máy tính của họ trong mạng.

MDNS:

1. Giải quyết tên máy tính: cho phép các thiết bị trong cùng một mạng cục bộ tự động giải quyết tên máy tính của họ thành địa chỉ IP.
2. Giải quyết tên dịch vụ: cũng cho phép các thiết bị tự động giải quyết tên các dịch vụ (service names) mà họ cung cấp, cũng như địa chỉ IP của dịch vụ đó.
3. Hỗ trợ mạng cục bộ: thường được sử dụng trong các mạng cục bộ, nơi các thiết bị kết nối trực tiếp vào mạng mà không có sự tham gia của máy chủ DNS trung gian.

4. Tích hợp dễ dàng: thường được tích hợp sẵn trong các hệ điều hành và phần mềm mạng cục bộ
5. Hỗ trợ cho các thiết bị IoT và mạng cục bộ phức tạp: rất hữu ích trong các mạng cục bộ có nhiều thiết bị IoT (Internet of Things) và trong các mô hình mạng cục bộ phức tạp, giúp các thiết bị này dễ dàng tìm kiếm và kết nối với nhau.

SSDP:

1. Tìm kiếm và khám phá dịch vụ: cho phép các thiết bị trong mạng cục bộ gửi các yêu cầu tìm kiếm (search requests) để khám phá các dịch vụ và thiết bị có sẵn trong mạng.
2. Đăng ký và thông báo dịch vụ: cho phép các thiết bị cung cấp dịch vụ đăng ký thông tin về dịch vụ của họ thông qua các thông báo (advertisement) multicast.
3. Tương tác với UPnP: thường được sử dụng trong kết hợp với UPnP (Universal Plug and Play), một chuẩn kỹ thuật cho phép các thiết bị tự động phát hiện và tương tác với nhau trong mạng cục bộ.
4. Hỗ trợ cho các ứng dụng mạng cục bộ: thường được sử dụng trong các ứng dụng mạng cục bộ như phương tiện truyền thông thông qua DLNA (Digital Living Network Alliance) hoặc trong các ứng dụng chia sẻ tập tin và máy in trong mạng nội bộ.

5. Tích hợp dễ dàng: thường được tích hợp vào các thiết bị mạng và phần mềm dễ dàng, và nó hoạt động tự động khi các thiết bị được kết nối vào mạng.

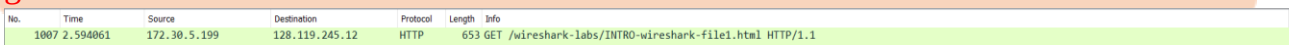
Câu 3: Có bao nhiêu gói tin HTTP? Tỉ lệ % số gói tin HTTP/Tổng số gói tin?

Có 2 gói tin HTTP. Tỉ lệ % số gói tin HTTP/Tổng số gói tin là 0.12%

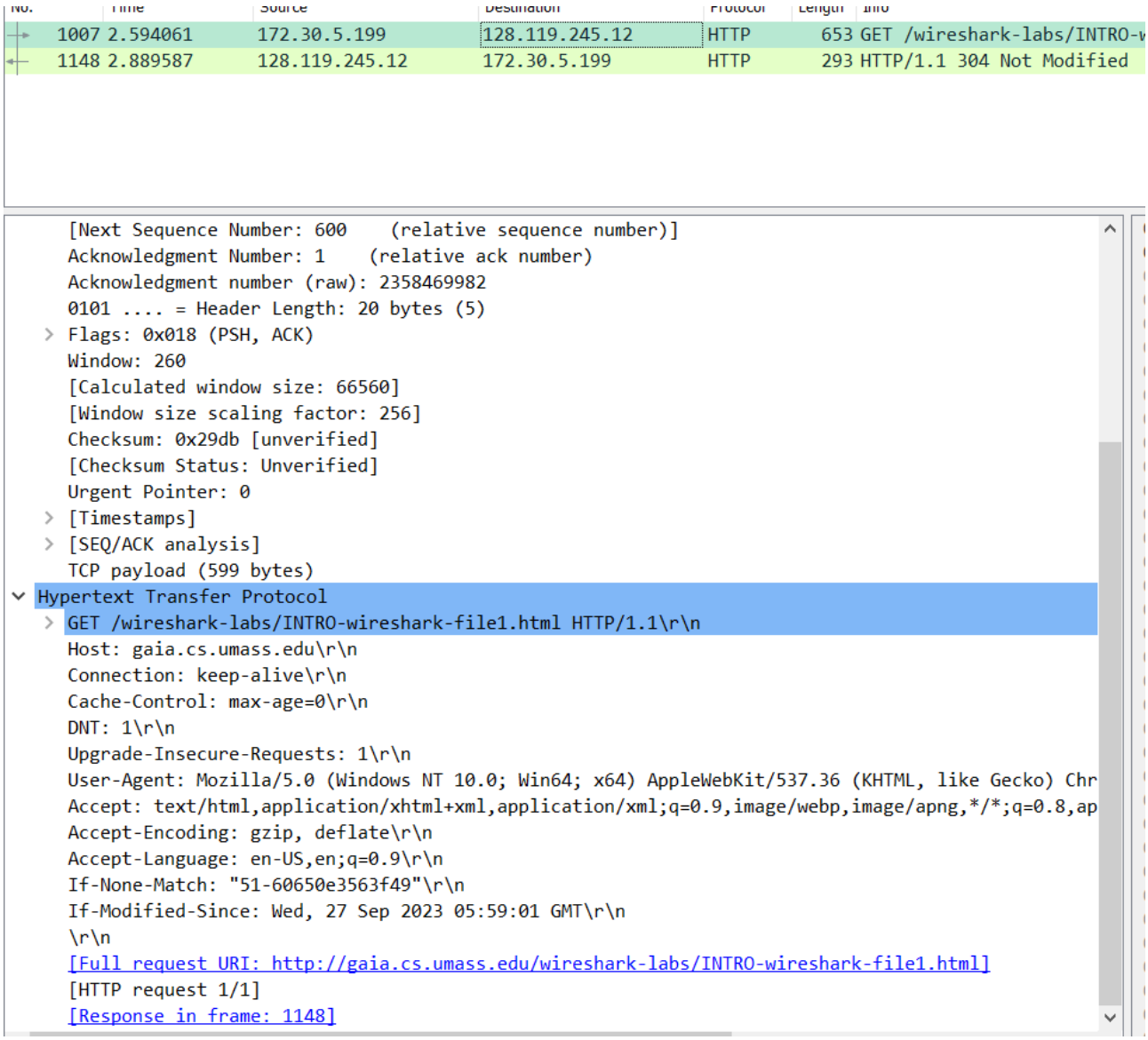
Câu 4: Có bao nhiêu gói tin HHTP GET?

Có 1 gói tin HTTP GET. Ta dựa vào cột info để tìm các gói GET

Câu 5: Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server gaia.cs.umass.edu?

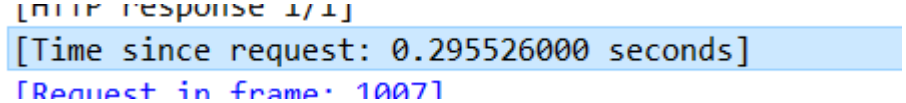


Câu 6: Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?



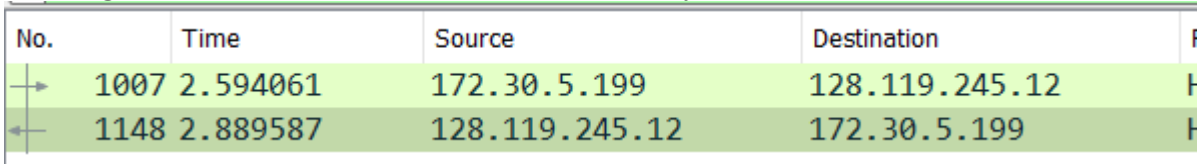
Câu 7: Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)?

Mất 0.295526000 từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6). Ta xác định dựa vào dòng Time since request trong cửa sổ Packet Details của gói tin ở câu 6



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?

IP của gaia.cs.umass.edu: 128.119.245.12. IP máy tính: 172.30.5.199



Ta dựa vào dòng Internet Protocol trong cửa sổ Packet Details của các gói tin HTTP . Dòng này có hiểu thị IP source (IP máy gửi tin) và IP Destination (IP máy đến), đối với gói tin HTTP GET thì IP source là IP máy chúng ta và IP Destination là IP của trang web, đối với gói tin phản hồi thì sẽ ngược lại.

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

Tổng số gói tin bắt được là 1501 mất 3.800433

	Time
1482	3.789736
1483	3.789736
1484	3.799781
1485	3.799781
1486	3.799781
1487	3.799781
1488	3.799781
1489	3.799781
1490	3.799781
1491	3.799781
1492	3.799781
1493	3.799781
1494	3.799781
1495	3.799781
1496	3.799781
1497	3.799781
1498	3.799781
1499	3.799781
1500	3.799781
1501	3.800433

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

QUIC:

1. Tăng tốc độ kết nối,sử dụng mã hóa đa luồng (multiplexing) để cho phép nhiều luồng dữ liệu chia sẻ cùng một kết nối
2. Mã hóa và bảo mật sử dụng mã hóa TLS (Transport Layer Security) để bảo vệ dữ liệu truyền qua mạng.
3. Điều chỉnh tốc độ được thiết kế để tự động điều chỉnh tốc độ truyền dữ liệu dựa trên điều kiện mạng thực tế.
4. Hỗ trợ đa phương tiện hỗ trợ truyền tải nhiều loại dữ liệu đa phương tiện như văn bản, hình ảnh, âm thanh, video và các ứng dụng trực tuyến khác.
5. Tích hợp với HTTP/3 thường được kết hợp với giao thức HTTP/3 để tạo ra HTTP/3 over QUIC (còn được gọi là HTTP/3.0).

6. Ứng dụng trong các dịch vụ trực tuyến thường được sử dụng trong các dịch vụ trực tuyến như trình duyệt web, ứng dụng di động, và các ứng dụng truyền dữ liệu trực tiếp như trò chơi trực tuyến và phát sóng video trực tiếp.

ARP:

1. Ánh xạ địa chỉ IP sang địa chỉ MAC cho phép thiết bị trong mạng cục bộ tìm hiểu địa chỉ MAC của một thiết bị khi biết địa chỉ IP của nó.
2. Cập nhật bản đồ ARP: Mọi thiết bị trong mạng cục bộ duy trì một bản đồ ARP (ARP cache) để lưu trữ thông tin ánh xạ giữa địa chỉ IP và địa chỉ MAC của các thiết bị khác trong mạng.
3. Giải quyết xung đột địa chỉ IP bằng cách kiểm tra xem một địa chỉ IP đã được ánh xạ sang địa chỉ MAC nào trong bản đồ ARP. Nếu đã có ánh xạ, thiết bị có thể sử dụng thông tin này.
4. Hoạt động trong mạng cục bộ nơi các thiết bị kết nối trực tiếp vào mạng và cần phải biết địa chỉ MAC của các thiết bị khác để truyền dữ liệu.
5. Cải thiện hiệu suất mạng: Sử dụng bản đồ ARP giúp tránh việc phải thực hiện yêu cầu ARP quá nhiều lần, làm giảm tải mạng và cải thiện hiệu suất.

UDP:

1. Truyền tải dữ liệu: cho phép truyền tải dữ liệu từ một máy tính đến máy tính khác trong mạng.
2. Truyền tải nhanh chóng: là một giao thức nhẹ và nhanh chóng vì nó không có các tiến trình phức tạp như TCP như thiết lập kết nối, duy trì trạng thái, và quá trình xác nhận.
3. Định dạng đơn giản: có cấu trúc gói tin đơn giản, bao gồm tiêu đề và dữ liệu.
4. Sử dụng trong ứng dụng cụ thể: thường được sử dụng trong các ứng dụng nơi tính tin cậy không cần thiết và tốc độ là quan trọng hơn, như trò chơi trực tuyến, streaming media, và VoIP (Voice over IP).

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 ?

No.	Time	Source	Destination	Protocol	Length	Info
703	1.885441	172.30.5.199	192.168.20.76	HTTP	578	GET / HTTP/1.1

IP của celuit.edu.vn:192.168.20.76. IP máy tính: 172.30.5.199
Ta dựa vào dòng Internet Protocol trong cửa sổ Packet Details của các gói tin HTTP . Dòng này có hiểu thị IP source (IP máy gửi tin) và IP Destination (IP máy đến), đối với gói tin HTTP GET thì IP source là IP máy chúng ta và IP Destination là IP của trang web, đối với gói tin phản hồi thì sẽ ngược lại

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 ?

Có tổng cộng 6 gói tin với khối lượng dữ liệu hơn 4kb

Address A	Address B	Packets	Bytes	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.30.5.199	192.168.20.76	6	4 kB	19	31.58%	3	2 kB	3	2 kB	1.881357	0.3996	32 kbps	39 kbps