



Lab 1

BÁO CÁO BÀI THỰC HÀNH SỐ 1

Làm quen với Wireshark

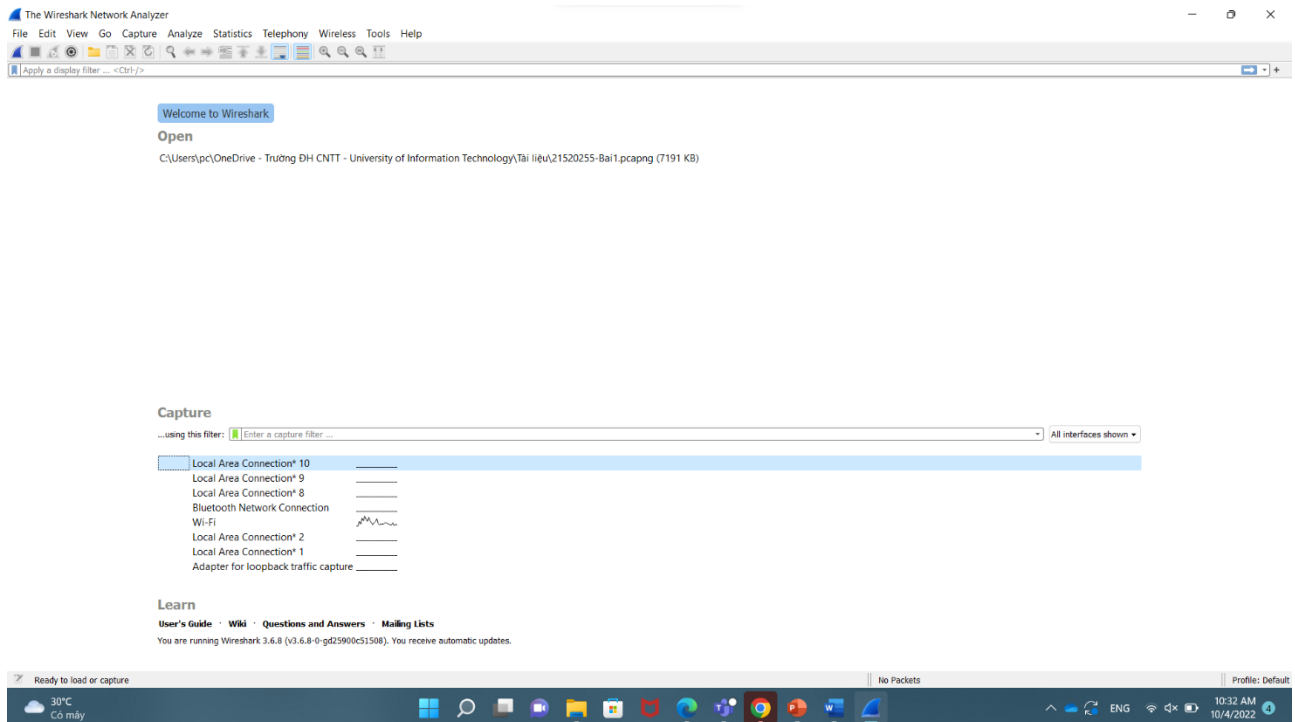
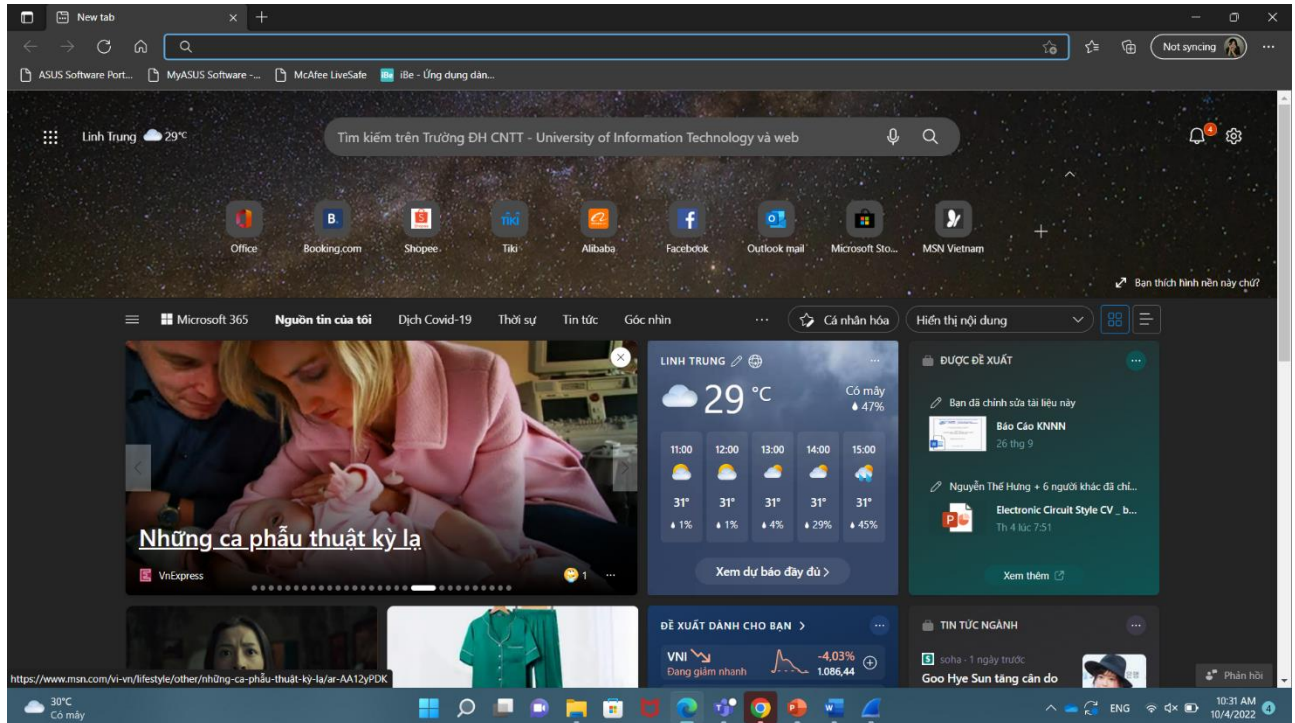
Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Giảng viên hướng dẫn	ThS. Đỗ Thị Hương Lan
Sinh viên thực hiện	Nguyễn Lê Quỳnh Hương (21520255)
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	21/09/2022 – 05/10/2022
Tự chấm điểm	9/10

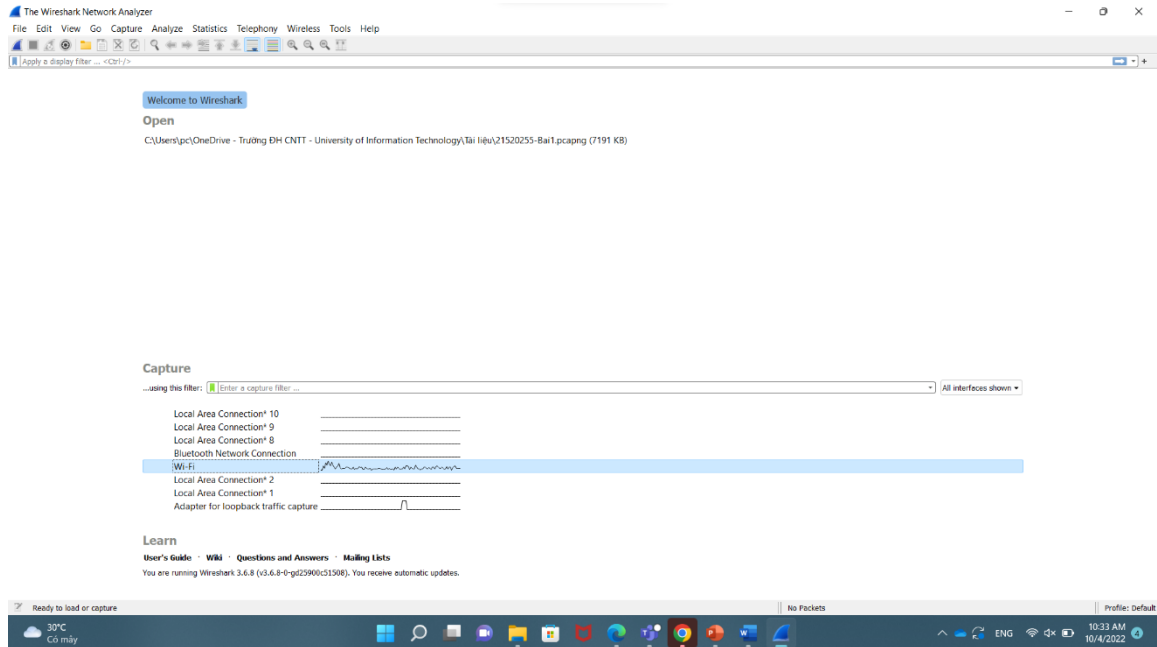
A. CÁC BƯỚC THỰC HÀNH

Bước 1: Khởi động trình duyệt web Google Chrome và phần mềm Wireshark (phiên bản mới nhất)

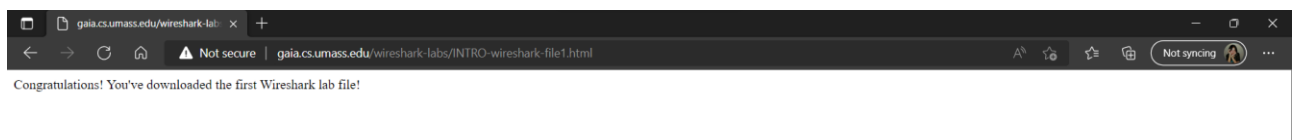


Lab 1: Làm quen với Wireshark

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

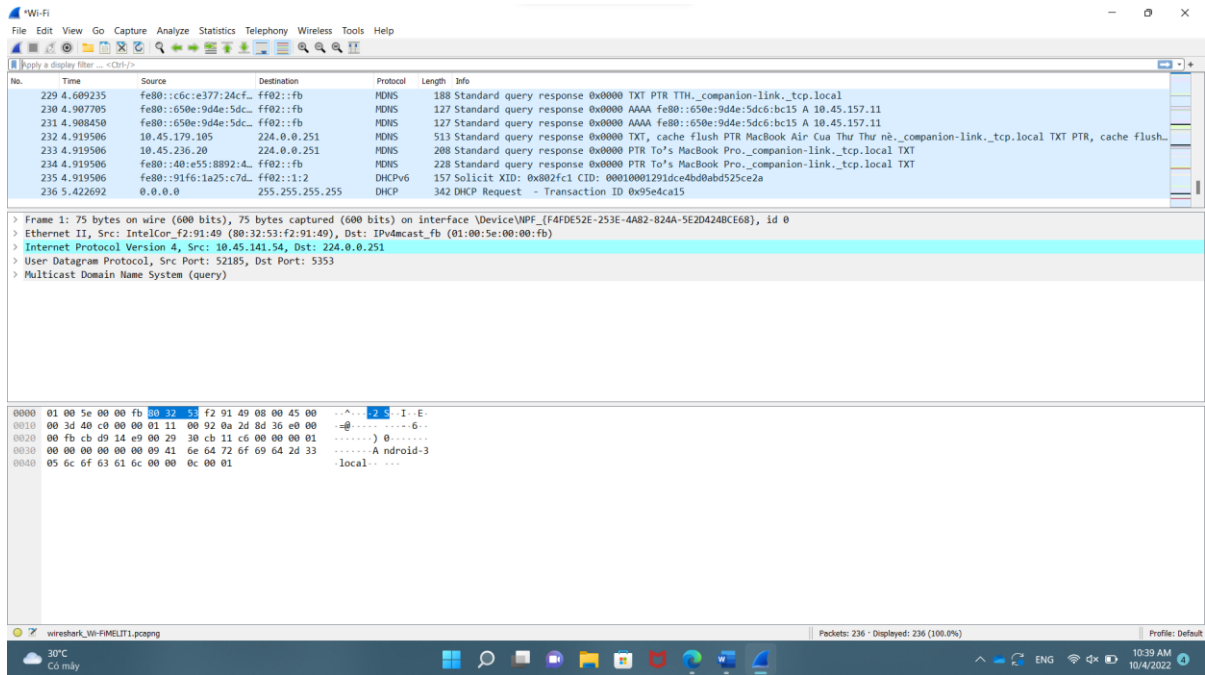


Bước 3: Sử dụng trình duyệt và chỉ truy cập vào website có địa chỉ như sau <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

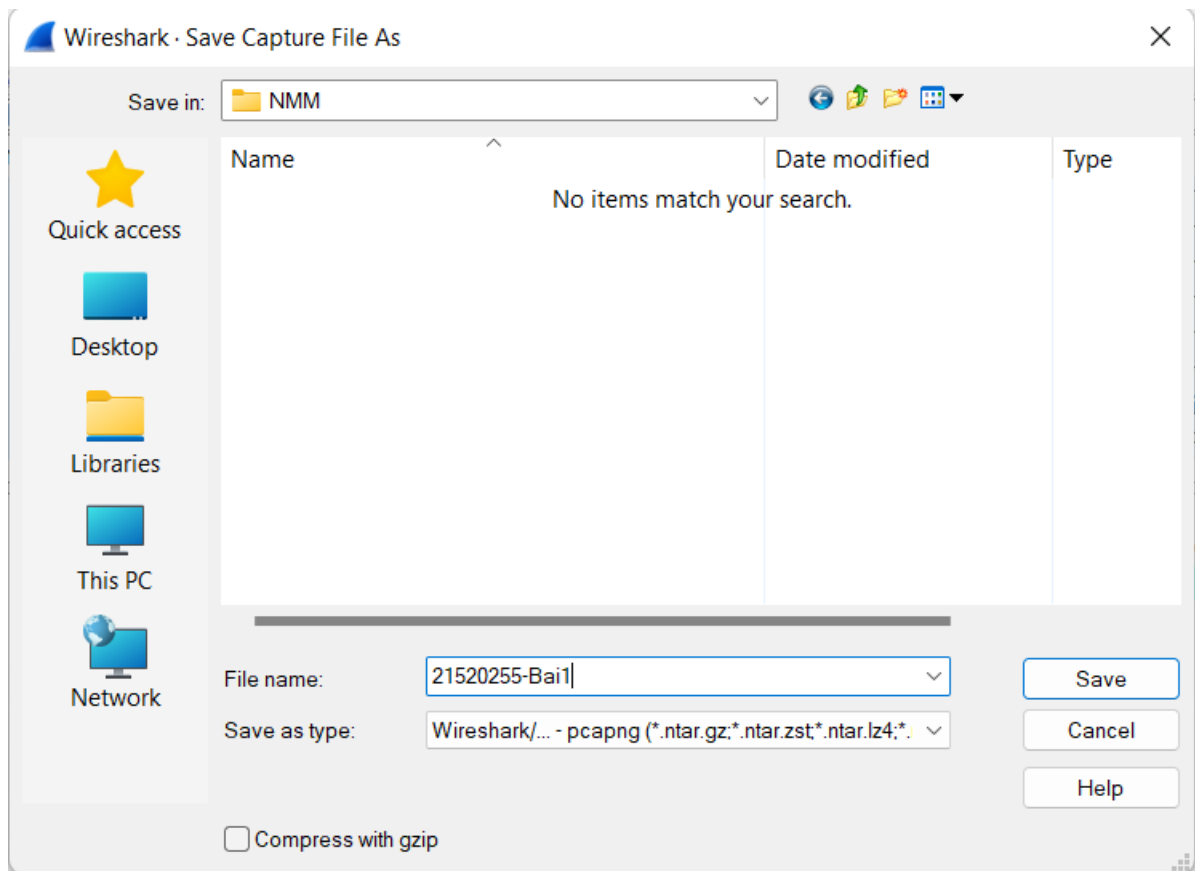


Bước 4: Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.

Lab 1: Làm quen với Wireshark



Bước 5: Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng 21520255-Bai1.pcapng.



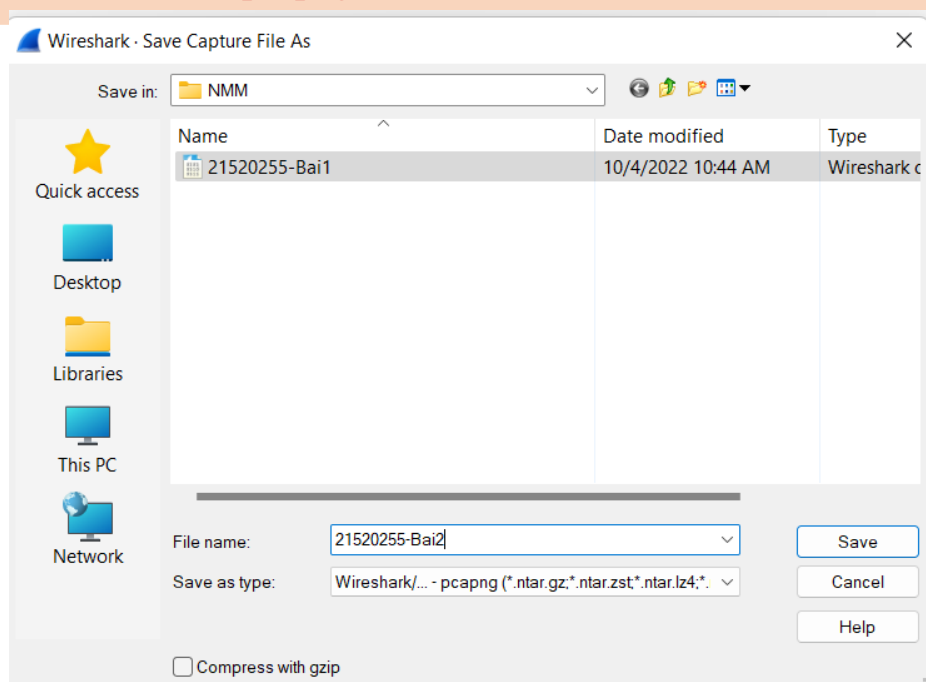
Lab 1: Làm quen với Wireshark

Bước 6: Chọn Start capturing packets để bắt đầu quá trình bắt gói tin mới.

Bước 7: Mở website <http://www.celuit.edu.vn> thực hiện lại Bước 4,5,6



Bước 8: Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên dạng 21520255-Bai2.pcapng



B. TRẢ LỜI CÁC CÂU HỎI

Task 1: Mở đầu về Mạng máy tính

Câu 1 : Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng tại nơi ở.

- Các loại thiết bị liên quan đến Mạng : Modem, Router, Repeater,...



Câu 2 : Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?

- Hiện nay, hàng loạt tập đoàn, doanh nghiệp, công ty, ngân hàng,... đều phụ thuộc vào Internet. Nếu như Internet biến mất trong 5 phút, sẽ không có bất cứ giao dịch ngân hàng quốc tế nào được thực hiện, những dây chuyền được điều khiển tự động sẽ dừng lại, năng suất làm việc sụt giảm. Quân đội sử dụng công nghệ cao có khả năng rối loạn do không nắm bắt được chỉ thị để phối hợp hoạt động. Ảnh hưởng đến kinh tế, các hoạt động giải trí online, mua sắm online.

Câu 3 : Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

- Hiểu được khái niệm, các phương diện áp dụng của các giao thức ứng dụng mạng, hiểu về các giao thức thông qua việc xem xét các giao thức phổ biến của lớp ứng dụng.
- Hiểu về các nguyên lý đằng sau các dịch vụ tầng Vận chuyển, hiểu về các giao thức tầng Vận chuyển trên Internet.
- Hiểu các nguyên lý nền tảng của các định vụ tầng Mạng và hiện thực trong Internet.

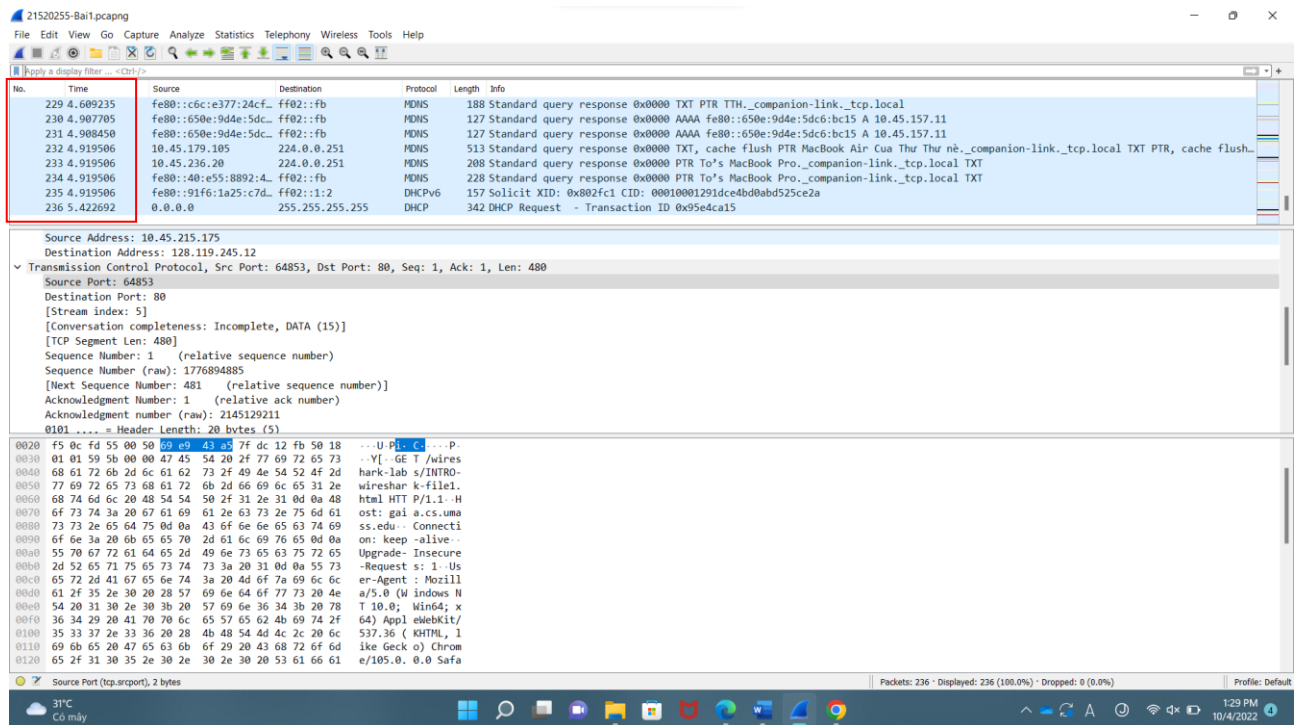
Lab 1: Làm quen với Wireshark

- Hiểu về các nguyên lý của các dịch vụ tầng Liên kết dữ liệu, khởi tạo và hiện thực một số công nghệ tầng Liên kết dữ liệu.

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

Câu 1:

- Quan sát dòng cuối của cột Time => tổng thời gian bắt gói tin là 5.422692
- Quan sát dòng cuối của cột No. => tổng số gói tin bắt được là 236



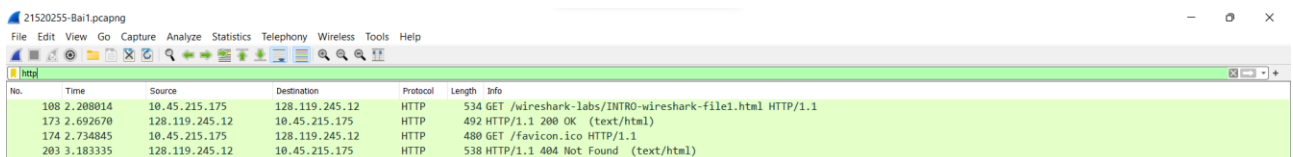
Câu 2:

- Quan sát cột protocol để xem các giao thức:
- **TCP : Transmission Control Protocol** là giao thức tiêu chuẩn trên Internet đảm bảo trao đổi thành công các gói dữ liệu giữa các thiết bị qua mạng. TCP là giao thức truyền tải cơ bản cho nhiều loại ứng dụng, bao gồm máy chủ web và trang web, ứng dụng email, FTP và các ứng dụng ngang hàng. Đây là một trong những giao thức được sử dụng phổ biến nhất trong truyền thông mạng kỹ thuật số và đảm bảo cung cấp dữ liệu đầu cuối.
- **DNS : Domain Name System** là hệ thống phân giải tên miền, nghĩa là khi muốn truy cập một thông tin thông qua tên miền thì DNS giúp chuyển tên miền thành địa chỉ IP tương ứng để trình duyệt có thể tải tài nguyên Internet. DNS có vai trò lớn trong liên kết các thiết bị mạng với nhau trong việc định vị và gán địa chỉ cụ thể cho các thông tin trên internet.
- **SSDP : Simple Service Discovery Protocol** là Giao thức khám phá dịch vụ đơn giản, là một giao thức mạng được sử dụng trong các mạng nhỏ, bao gồm cả mạng gia đình, để quảng cáo và khám phá các dịch vụ mạng chủ yếu được hỗ trợ bởi kiến trúc Universal Plug-and-Play (UPnP). SSDP là một giao thức văn bản dựa trên HTTPU sử dụng XML. Nó trao đổi tin nhắn bằng cách sử dụng gói dữ liệu UDP.
- **DHCP : Dynamic Host Configuration Protocol** là Giao thức cấu hình máy chủ, có nhiệm vụ giúp quản lý nhanh, tự động và tập trung việc phân phối địa chỉ IP bên trong một mạng. DHCP tự động hóa và quản lý tập trung các cấu hình này thay vì yêu cầu quản trị viên mạng gán thủ công địa chỉ IP cho tất cả các thiết bị mạng.

Protocol
MDNS
MDNS
MDNS
TCP
HTTP
HTTP
IPv4
MDNS

Câu 3:

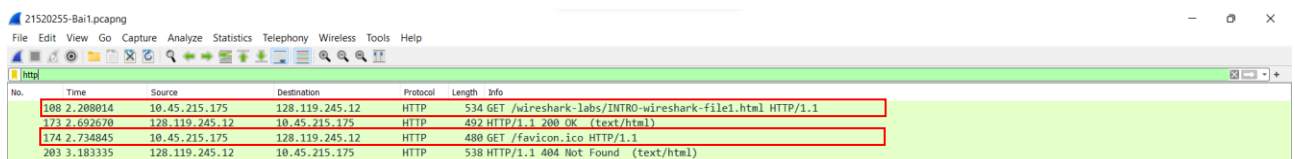
- Số gói tin HTTP: 4
- Tỷ lệ số gói tin HTTP/Tổng gói tin: 4/236



No.	Time	Source	Destination	Protocol	Length	Info
108	2.2088014	10.45.215.175	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
173	2.692670	128.119.245.12	10.45.215.175	HTTP	492	HTTP/1.1 200 OK (text/html)
174	2.734845	10.45.215.175	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
203	3.183335	128.119.245.12	10.45.215.175	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Câu 4:

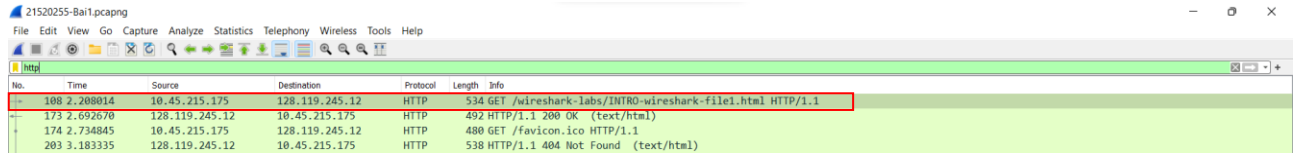
- Có 2 gói tin HTTP GET



No.	Time	Source	Destination	Protocol	Length	Info
108	2.2088014	10.45.215.175	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
173	2.692670	128.119.245.12	10.45.215.175	HTTP	492	HTTP/1.1 200 OK (text/html)
174	2.734845	10.45.215.175	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
203	3.183335	128.119.245.12	10.45.215.175	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Câu 5:


- Gói tin HTTP GET đầu tiên được gửi đến web server là:



The screenshot shows the Wireshark interface with a packet list table. The first packet is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
108	2.208014	10.45.215.175	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
173	2.692670	128.119.245.12	10.45.215.175	HTTP	492	HTTP/1.1 200 OK (text/html)
174	2.734845	10.45.215.175	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
203	3.183335	128.119.245.12	10.45.215.175	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- Quan sát cửa sổ packet details mục Host sẽ biết được web server và HTTP request 1/2 để biết đây là gói tin HTTP GET đầu tiên trên tổng số 2 gói tin HTTP GET.

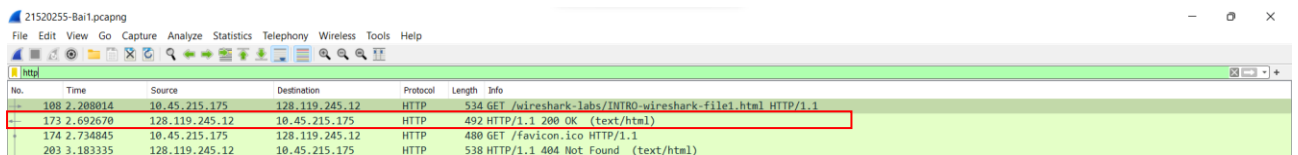


The screenshot shows the packet details pane for the first packet. The 'Host' field is highlighted with a red box.

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.53\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 173]
[Next request in frame: 174]
```

Câu 6:

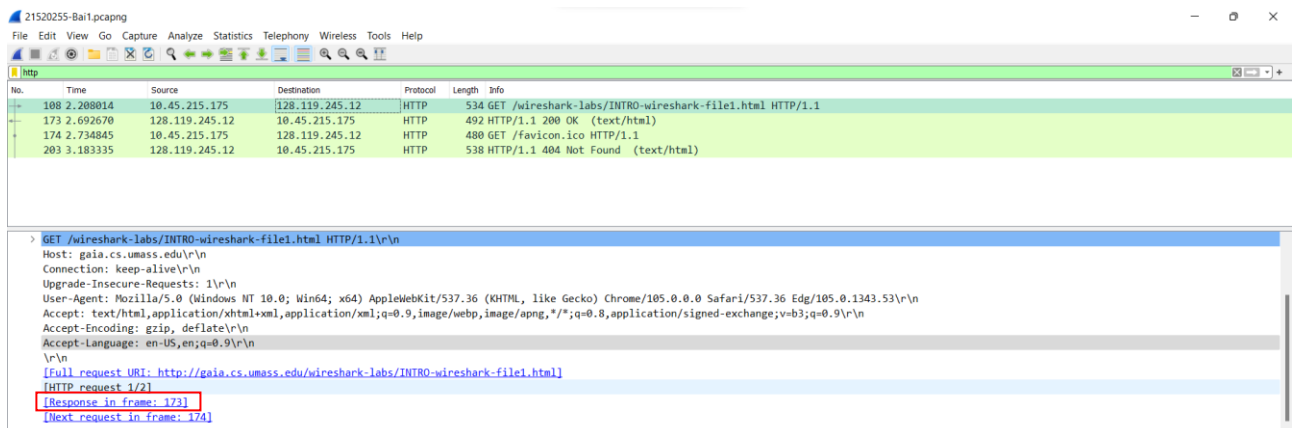
- Gói tin phản hồi cho gói HTTP GET ở câu 5 là:



The screenshot shows the Wireshark interface with a packet list table. The second packet is highlighted with a red box.

No.	Time	Source	Destination	Protocol	Length	Info
108	2.208014	10.45.215.175	128.119.245.12	HTTP	534	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
173	2.692670	128.119.245.12	10.45.215.175	HTTP	492	HTTP/1.1 200 OK (text/html)
174	2.734845	10.45.215.175	128.119.245.12	HTTP	480	GET /favicon.ico HTTP/1.1
203	3.183335	128.119.245.12	10.45.215.175	HTTP	538	HTTP/1.1 404 Not Found (text/html)

- Quan sát giá trị Response in Frame để biết số thứ tự gói tin phản hồi cho gói HTTP GET ở câu 5. Ở đây ta có số thứ tự gói tin phản hồi là 173.



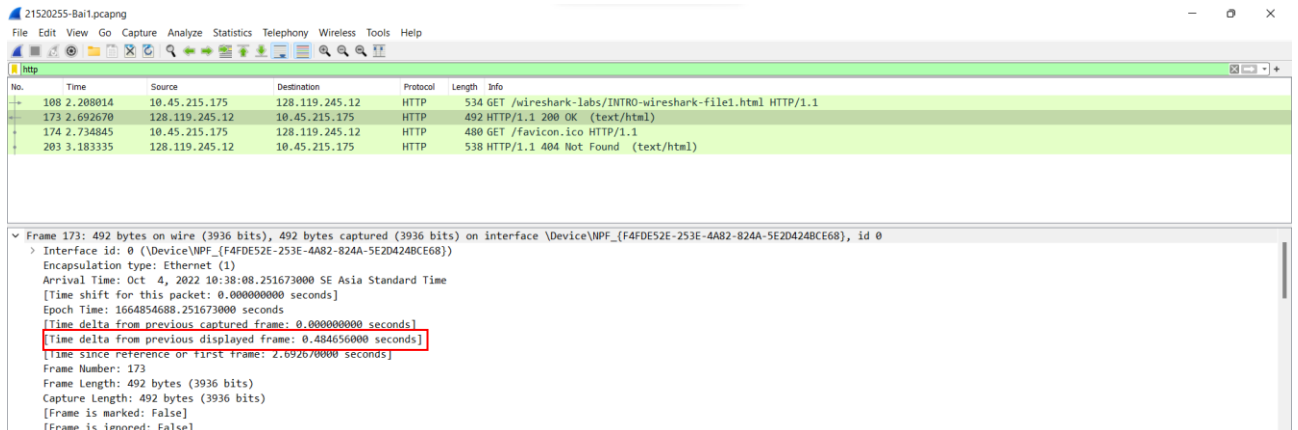
The screenshot shows the packet details pane for the first packet. The 'Response in frame: 173' field is highlighted with a red box.

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.53\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 173]
[Next request in frame: 174]
```

Lab 1: Làm quen với Wireshark

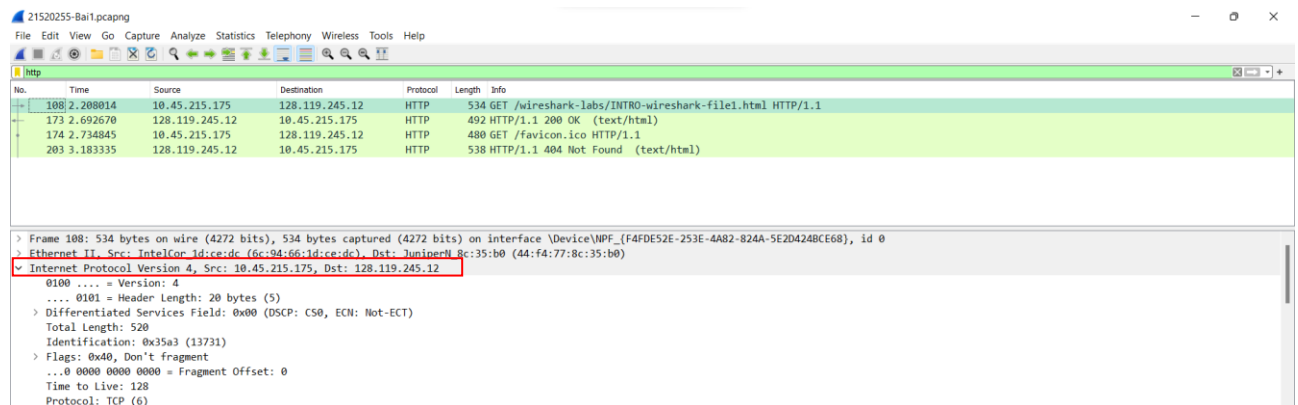
Câu 7:

- Quan sát thời gian từ lúc gửi gói tin HTTP GET ở câu 5 đến khi nhận được gói tin phản hồi ở câu 6 ở cửa sổ chi tiết gói tin: Thời gian là 0.484656s



Câu 8:

- Quan sát mục IP version 4 để biết địa chỉ IP
 - Địa chỉ IP của gaia.cs.umass.edu là: 128.119.245.12
 - Địa chỉ IP của máy tính đang sử dụng là: 10.45.215.175

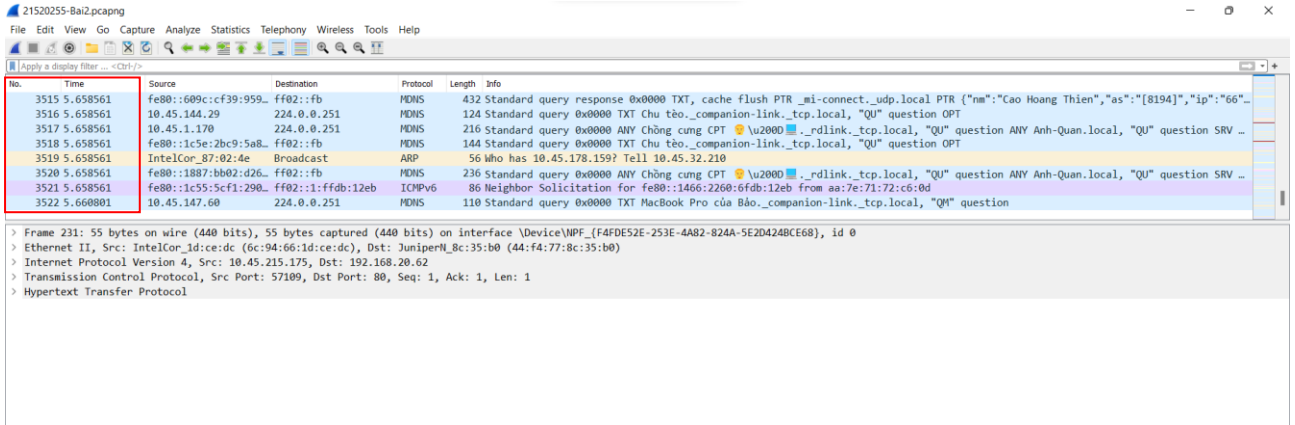


- Giải thích: Trình duyệt trên máy tính cá nhân yêu cầu, Web server phản hồi.

Câu 9:

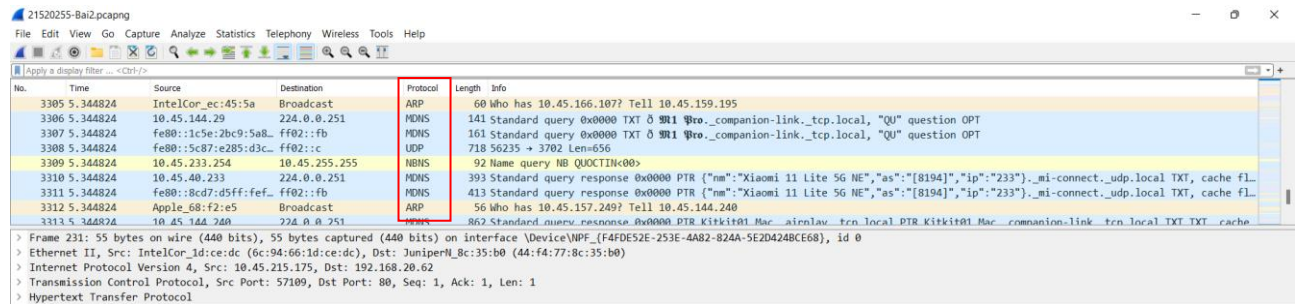
- Quan sát cột No. và Time:
 - Tổng thời gian bắt gói tin là: 5.660801s
 - Tổng số gói tin bắt được là: 3522

Lab 1: Làm quen với Wireshark



Câu 10:

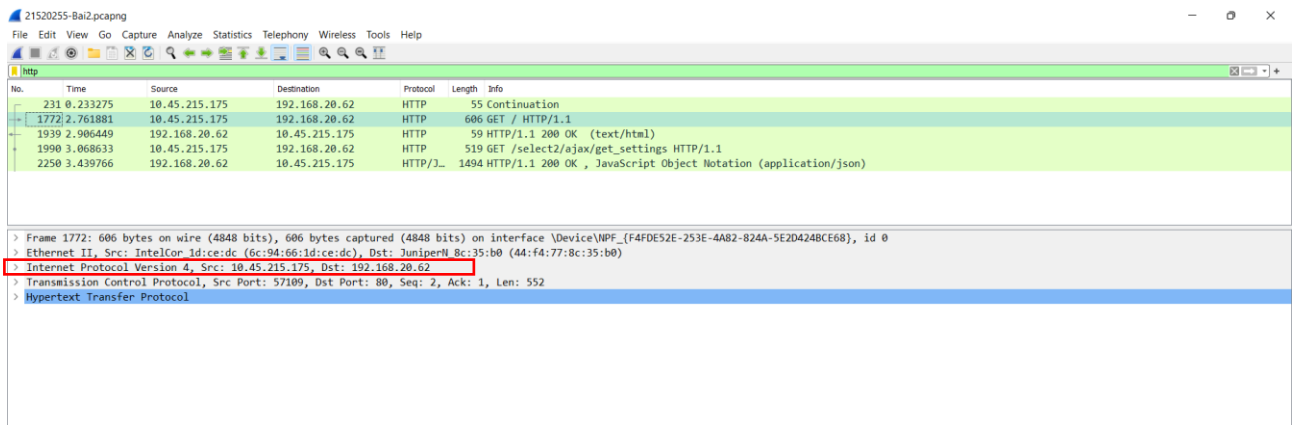
- 3 giao thức khác nhau xuất hiện trong cột giao thức là:
 - NBNS : **NetBIOS Name Service** là một giao thức mạng được tạo ra cho các hệ thống cũ để cho phép giao tiếp qua các mạng TCP/IP hiện đại. Trong nhiều trường hợp NBNS vẫn được sử dụng trong một số tổ chức ngày nay, việc vô hiệu hóa nó có thể gây ra sự gián đoạn dịch vụ. Nó có nhiều chức năng giống như DNS cho phép các hệ thống kế thừa và phân giải DNS thành địa chỉ IP.
 - UDP : **User Datagram Protocol** là một trong những giao thức cốt lõi của giao thức TCP/IP. Chương trình có thể gửi những datagram tới máy khác. Các gói dữ liệu có thể đến không đúng thứ tự hoặc bị mất mà không có thông báo. UDP nhanh và hiệu quả hơn đối với các mục tiêu như kích thước nhỏ và yêu cầu khắt khe về thời gian, hữu dụng đối với việc trả lời các truy vấn nhỏ với số lượng lớn người yêu cầu.
 - ARP : **Address Resolution Protocol** 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 11:

- Địa chỉ IP trang web đã chọn ở celuit.edu.vn là: 192.168.20.62



Câu 12:

- Số lượng gói tin: 23
- Khối lượng dữ liệu được trao đổi: 15kbytes

