

Họ và tên: Nguyễn Tuấn Vũ

Lớp: 10ĐH\_TMĐT

MSSV: 1050070053

# **LAB 1: LÀM QUEN VỚI WIRESHARK**

## B. THỰC HÀNH

### 1. Task 1: Mở đầu về Mạng máy tính

➡ Trước khi bắt đầu thực hành, sinh viên hãy trả lời các câu hỏi sau:

- Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng (kèm ảnh minh họa).
- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?
- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

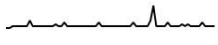
### 2. Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

#### 2.1 Giới thiệu và làm quen với Wireshark

Wireshark là phần mềm bắt gói tin (packet sniffer) rất phổ biến và miễn phí chạy trên Windows, Linux, MacOS, hỗ trợ bắt gói tin và quan sát nội dung của các thông điệp được trao đổi bởi các giao thức tại các tầng mạng khác nhau.

Ngoài ra, Wireshark còn phục vụ cho việc điều tra các chứng cứ số (forensic) liên quan đến các vụ án về mạng máy tính.

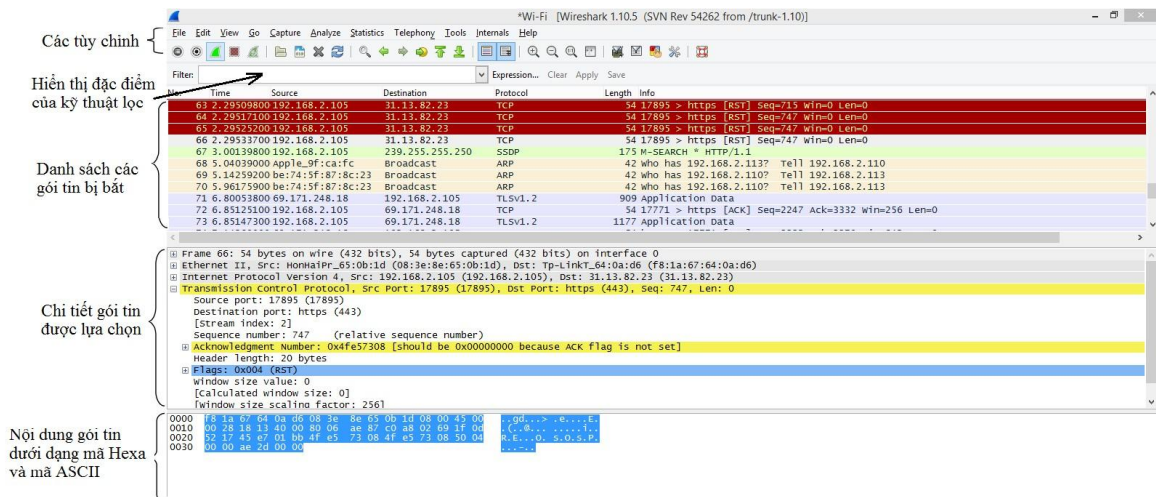
Giao diện chính khi mở Wireshark sẽ giống Hình 1.

Tại cửa sổ đầu tiên, bạn sẽ thấy danh sách các card mạng (hay network interface) trong mục Capture. Quan sát bên phải tên interface sẽ có minh họa thể hiện cho hoạt động trao đổi dữ liệu trong mạng, khi có dấu hiệu như  thì có thể nhận định đang có dữ liệu trao đổi qua interface đó.

Tùy theo loại kết nối và hệ điều hành đang sử dụng, tên của các interface sẽ khác nhau. Ví dụ, tên các interface thông thường trên Windows như sau:

- Kết nối có dây: Ethernet, Local Area Connection (LAN).
- Kết nối không dây: WiFi.

Sau đó, giao diện bắt gói tin sẽ xuất hiện như sau.



Hình 2. Giao diện chính của Wireshark trong suốt quá trình bắt và phân tích gói tin

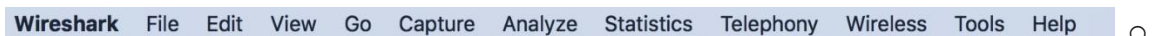
Lưu ý: Để có thể bắt được các gói tin đi qua nó, card mạng cần được kích hoạt chế độ Promiscuous (mặc định sẽ được kích hoạt sẵn trong Wireshark)







Hình 3. Có thể vào Capture > Options để theo dõi cài đặt trên từng interface

Giao diện Wireshark gồm có 5 thành phần chính từ trên xuống:

1. Command menus: chứa các menu thực hiện các chứng năng chính của Wireshark. Chúng ta quan tâm chủ yếu đến File và Capture.

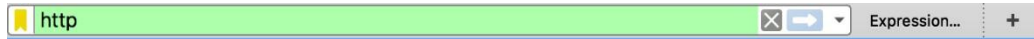


File menu chứa các tùy chọn cho phép lưu các gói tin đã bắt được (Save) dưới dạng file .pcapng hoặc mở file chứa các gói tin đã bắt từ trước. ○ Capture menu cho phép bắt đầu bắt gói tin và thay đổi các tùy chỉnh ○ Các button thường dùng:

-  - Bắt đầu bắt gói tin trên card mạng đã chọn.
-  - Dừng quá trình bắt gói tin
-  - Khởi động lại quá trình bắt gói tin hiện tại
-  - Mở Capture Options để thay đổi các tùy chỉnh

2. Packet-display filter: Tên giao thức và các thông tin khác có thể được nhập vào đây để lọc các gói tin trong packet-listing window.

Ví dụ, để lọc các gói tin HTTP (các gói tin liên quan đến việc truy cập web), ta gõ "http" vào khung này và chọn Apply.



### 3. Packet-listing windows:

Hiển thị thông tin tóm tắt cho các gói tin đã bắt, bao gồm: ○ No: Số thứ tự (số này được gán bởi Wireshark, không phải số thứ tự chứa trong header của gói tin)

- Time: mốc thời gian gói tin bị bắt.
- Source: địa chỉ nguồn
- Destination: địa chỉ đích.
- Protocol: loại giao thức, chỉ hiển thị giao thức hoạt động ở tầng cao nhất.
- Length: độ dài (kích thước) gói tin.
- Info thông tin đặc tả cho giao thức đó.

### 4. Packet details window:

Cung cấp các thông tin chi tiết về gói tin được chọn từ packet-listing window.

```

▶ Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: Apple_c4:ae:ed (ac:bc:32:c4:ae:ed), Dst: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0)
▶ Internet Protocol Version 4, Src: 192.168.5.58, Dst: 64.233.188.95
▼ Transmission Control Protocol, Src Port: 52702, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 52702
  Destination Port: 443
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x010 (ACK)

```

Các thông tin này bao gồm chi tiết về Ethernet frame (giả sử gói tin được gửi và nhận thông qua Ethernet interface), IP datagram, TCP hoặc UDP segment và cuối cùng là thông tin về giao thức ở tầng cao nhất.

### 5. Packet Raw data

Hiển thị toàn bộ nội dung của gói tin dưới dạng ASCII và hexadecimal.

0000	18 66 da 02 c9 f0 ac bc 32 c4 ae ed 08 00 45 00	·f· · · · · 2 · · · · · E ·
0010	00 38 f3 ee 00 00 40 01 fa ec c0 a8 05 3a c0 a8	·8 · · · @ · · · · · : · ·
0020	05 5f 03 03 2f bf 00 00 00 00 45 00 00 38 3f 6d	·_ · · · / · · · · · E · · 8?m
0030	00 00 80 11 6f 5e c0 a8 05 5f c0 a8 05 3a c5 13	· · · · · 0 ^ · · · · · _ · · · · ·
0040	08 06 00 24 00 00	· · · \$ · ·

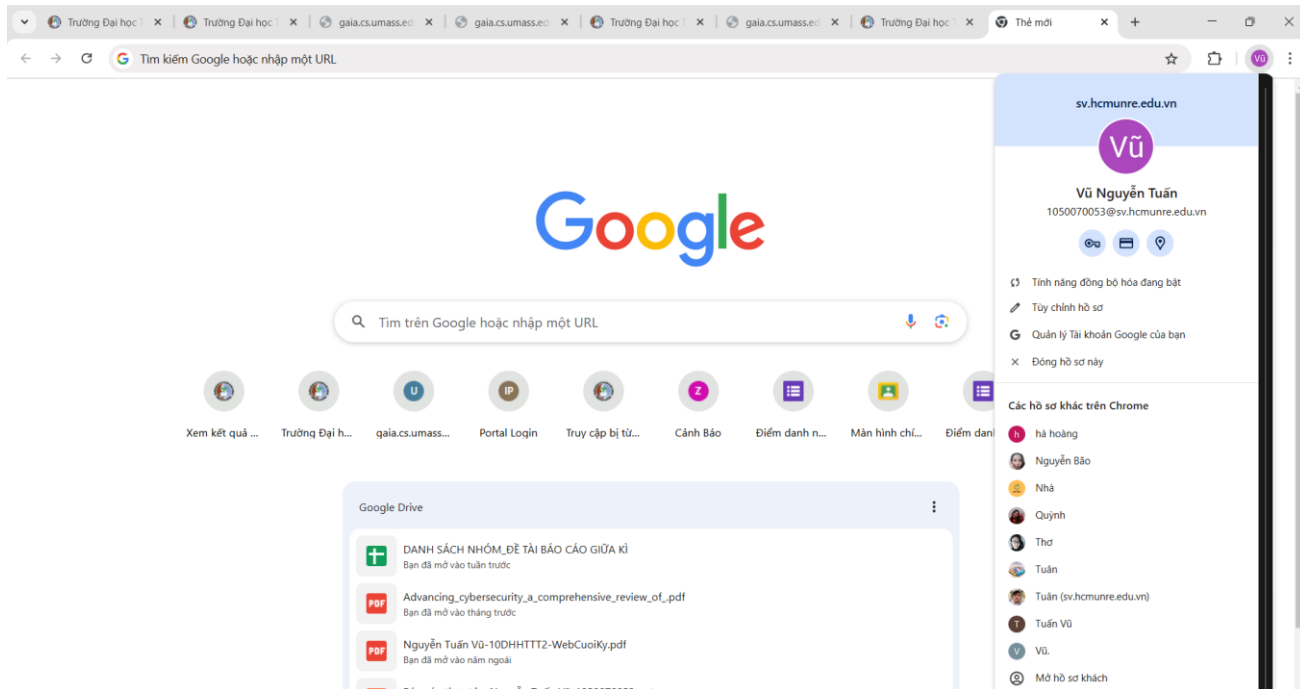
Thực ra, bản chất của mỗi gói tin bắt được chính là phần dữ liệu thô này. Các nội dung hiển thị tại phần 3, 4 do Wireshark phân tích và trực quan hóa để người dùng thuận tiện theo dõi.

## 2.2 Thử nghiệm bắt gói tin với Wireshark

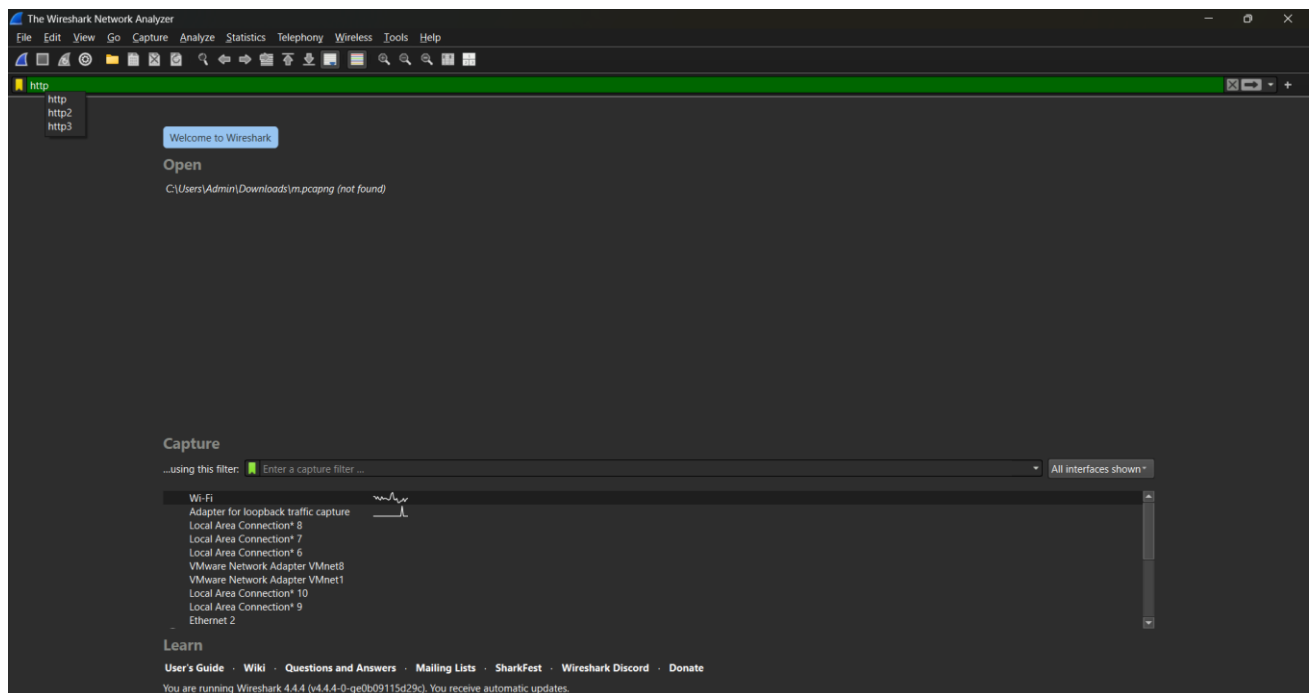
➔ Sinh viên thực hành theo các bước sau tại môi trường đã chuẩn bị:

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

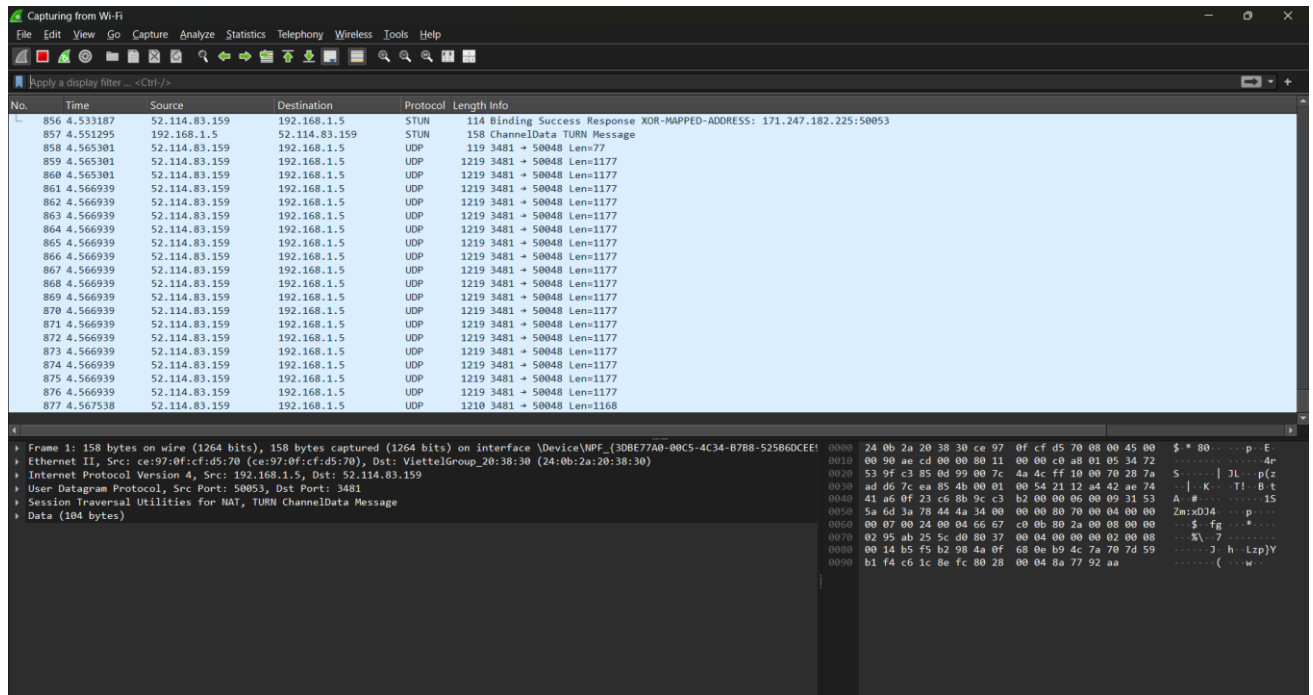
Lưu ý: Nếu sử dụng Wireshark cài đặt sẵn trong các máy tính tại phòng Lab, hãy kiểm tra và cập nhật Wireshark lên phiên bản mới nhất trước khi thực hành.



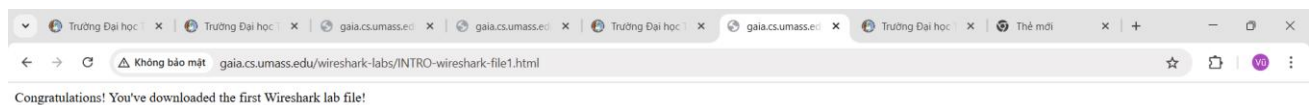
- Bước 2: Tại phần Capture, chọn interface đang hoạt động chính trên máy để bắt đầu bắt gói tin.



- Bước 3: Sau đó, cửa sổ như Hình 4 sẽ xuất hiện và hiển thị kết quả bắt gói tin tại interface đã chọn.

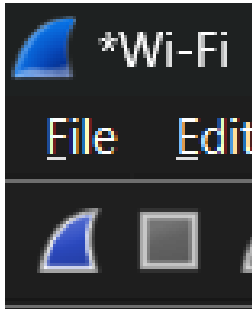


- Bước 4: Mở trình duyệt web và chỉ truy cập vào website có địa chỉ như sau <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> Đây là một website đơn giản có nội dung như sau:



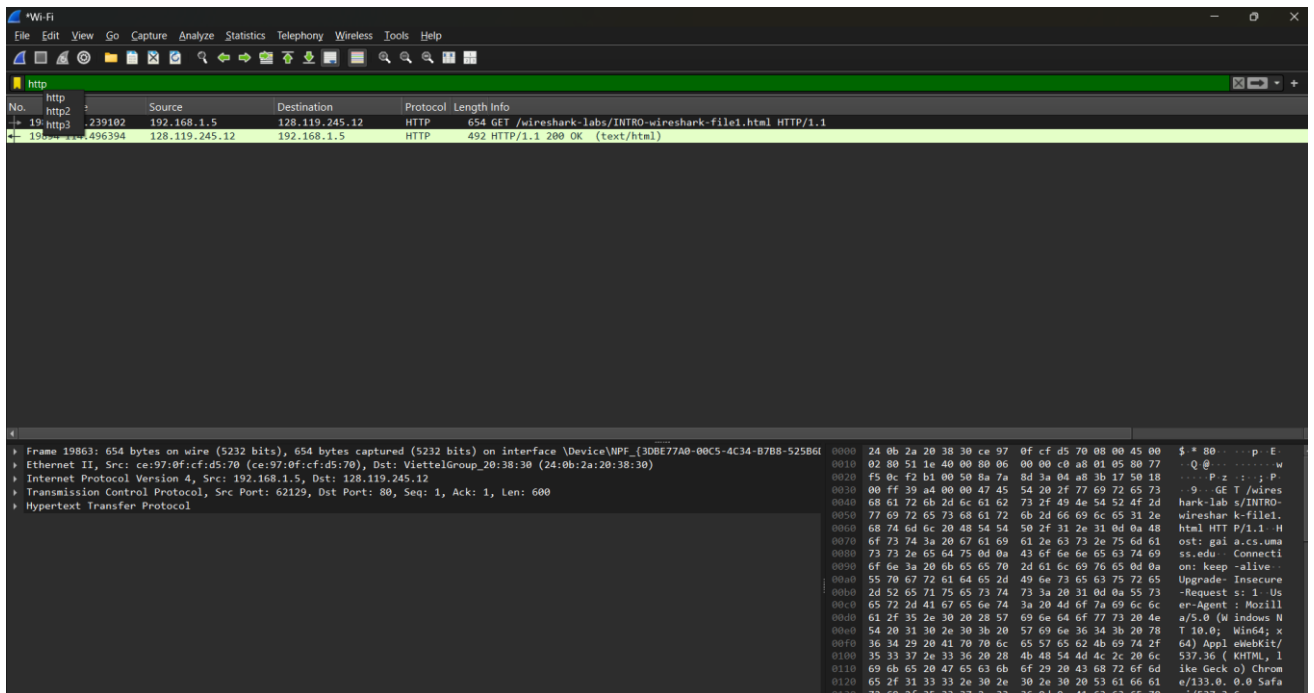
Hình 5. Truy cập website wireshark-file1 thành công

- **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.



Hình 6. Kết quả bắt gói tin sau khi dừng bắt gói tin

- **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.



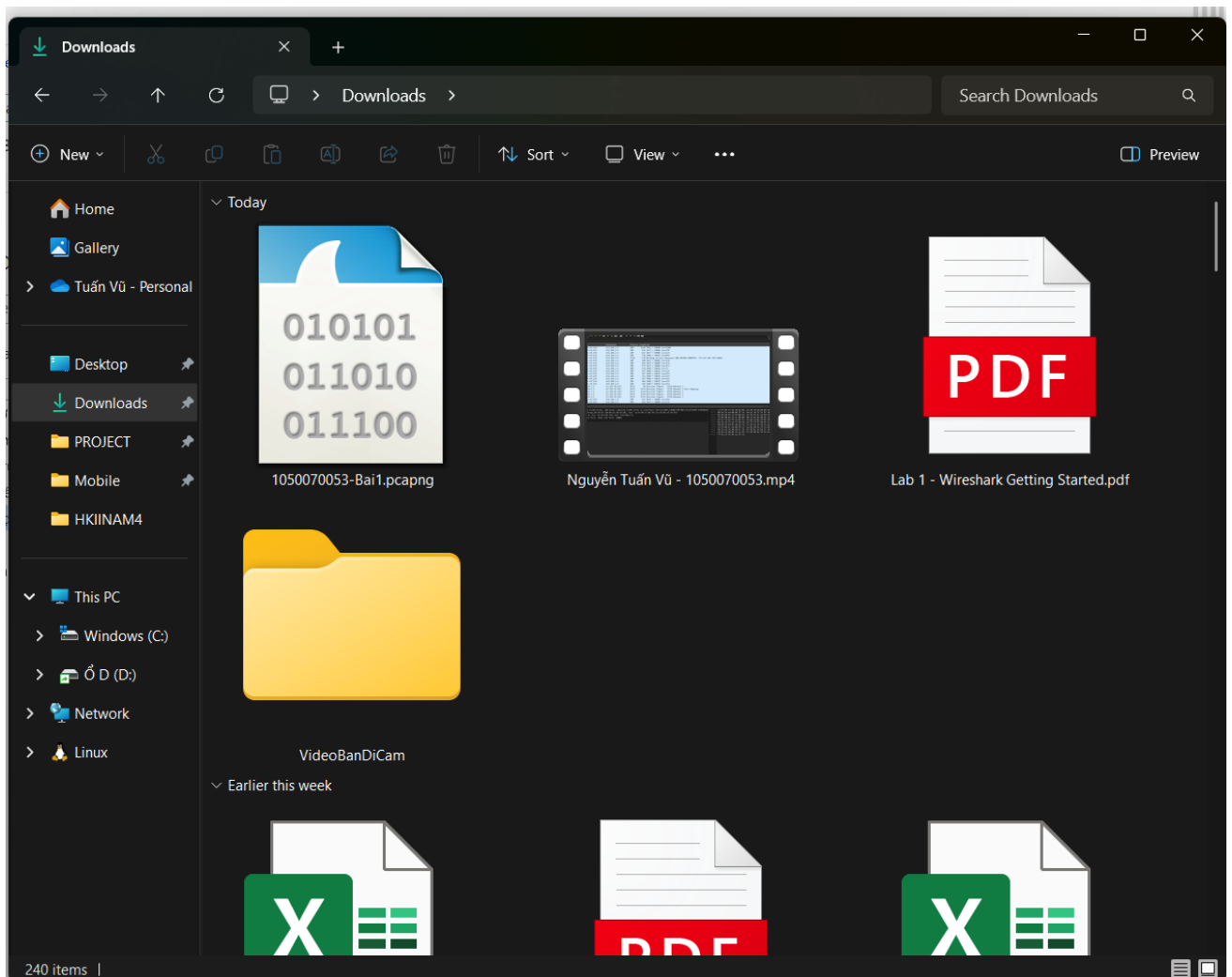
Hình 7. Lọc các gói tin HTTP từ kết quả bắt gói tin

- **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.

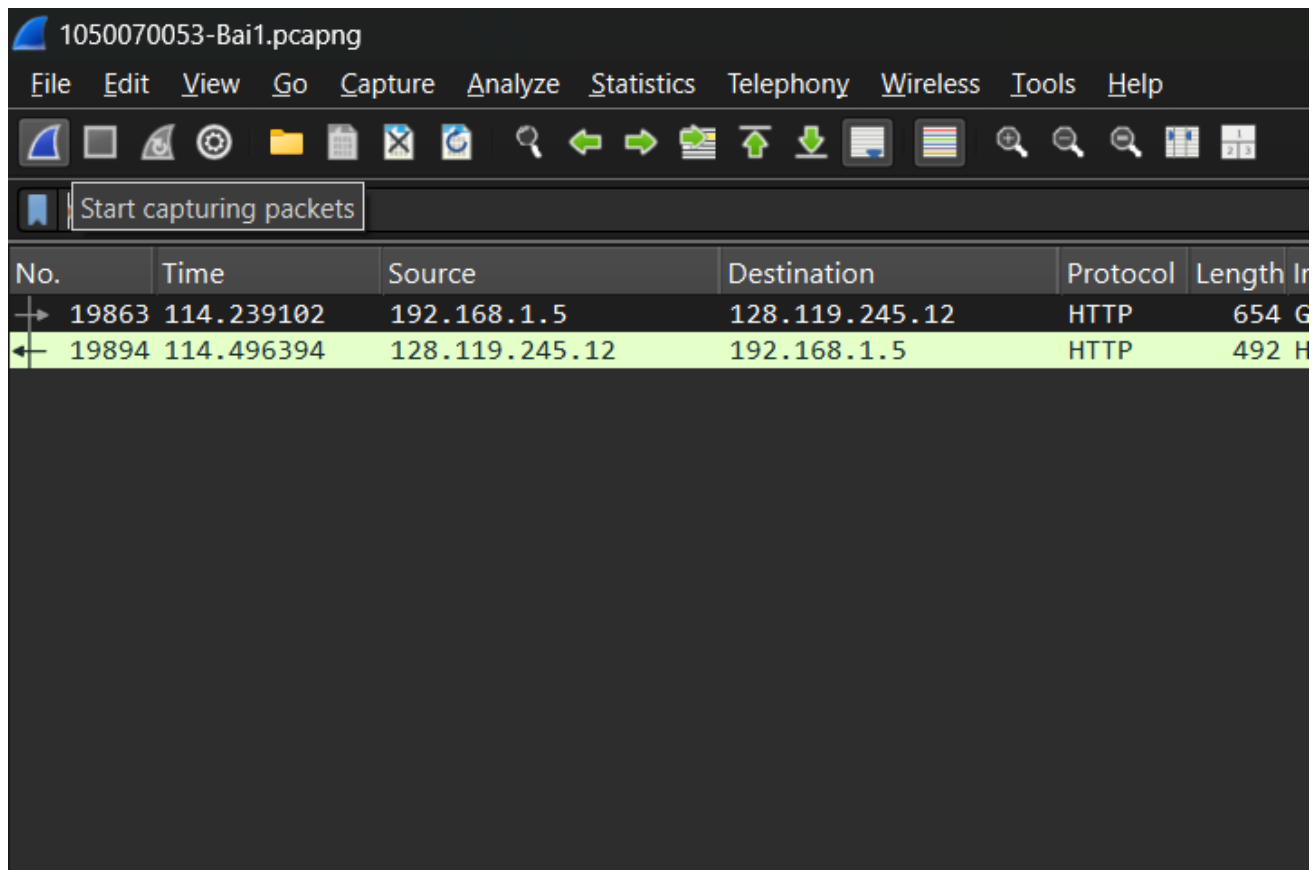
**Lưu ý:** Gói tin trả về HTTP – 200 OK chỉ xuất hiện khi bắt gói tin ở lần truy cập đầu tiên trên trình duyệt.

- **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.



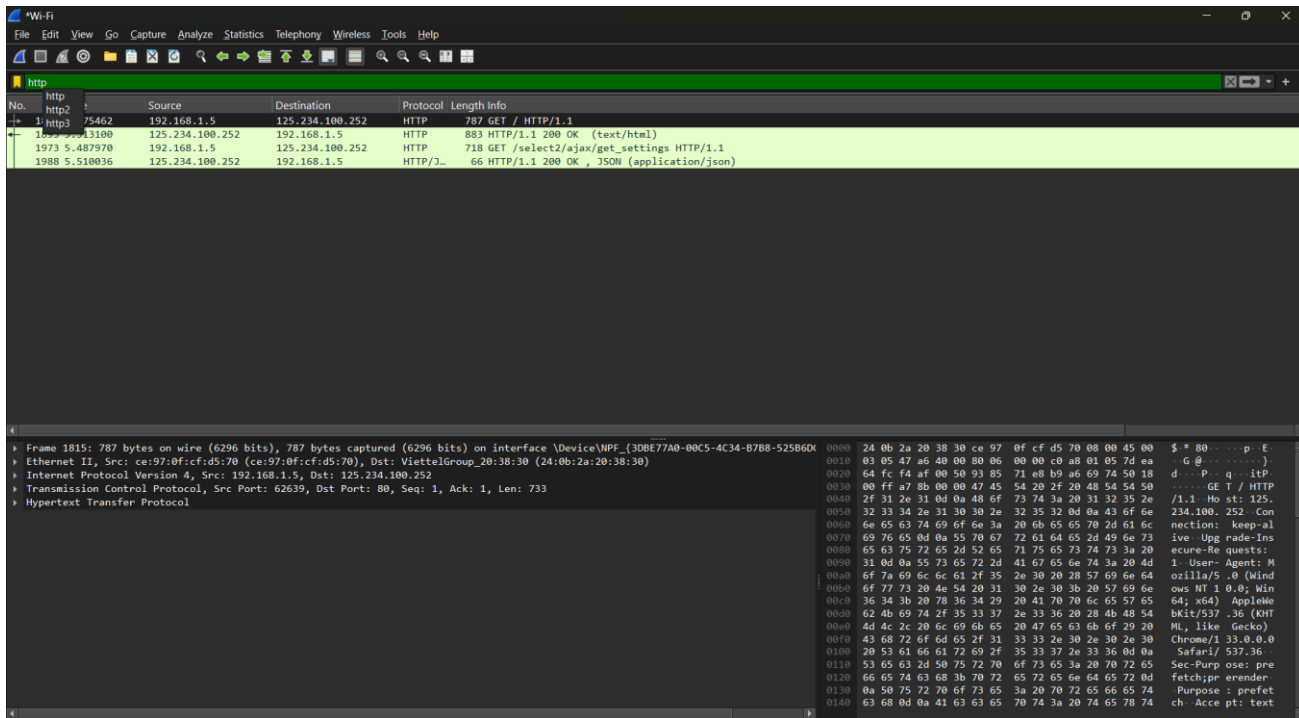


- **Bước 10:** Chọn 1 website mà sinh viên thường hay truy cập, ví dụ uit.edu.vn, tinhte.vn,... và tiến hành bắt gói tin trên website đó

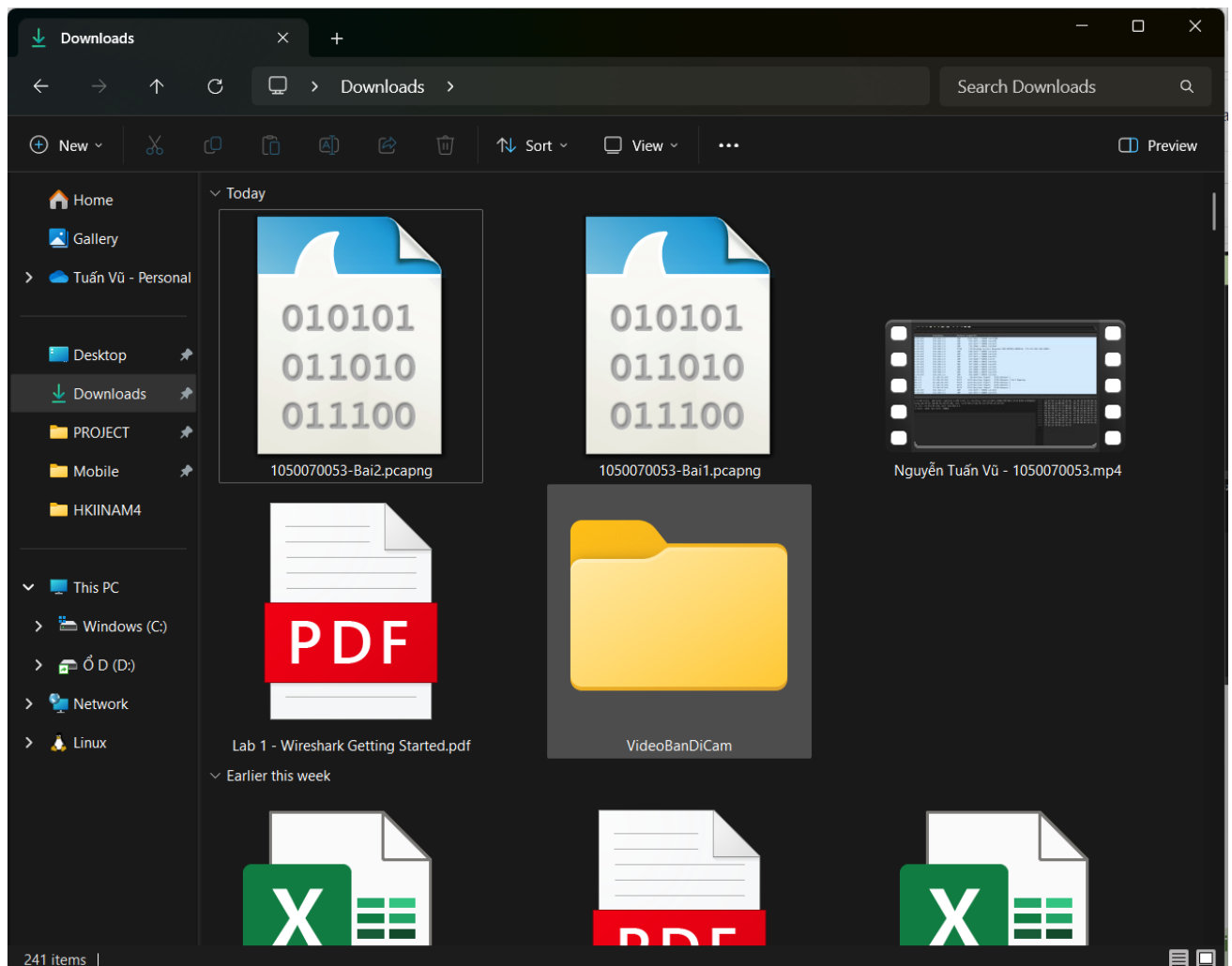
Lặp lại các bước 4-5-6-7 với một website khác có chứa nhiều thông tin hơn mà sinh viên thường truy cập. Ví dụ: tuoitre.vn, uit.edu.vn,...

- Ở đây em chọn website: <https://daotao.hcmunre.edu.vn/>

Tiến hành bắt gói tin tương tự:



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



### 2.3 Phân 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?

Trang web 1: Bắt được 20411 gói tin

Tổng thời gian: 117.32s



```
Arrival Time: Feb 28, 2025 13:47:08.069316000 SE Asia Standard Time
UTC Arrival Time: Feb 28, 2025 06:47:08.069316000 UTC
Epoch Arrival Time: 1740725228.069316000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.089748000 seconds]
[Time delta from previous displayed frame: 0.089748000 seconds]
[Time since reference or first frame: 117.320624000 seconds]
Frame Number: 20411
Frame Length: 114 bytes (912 bits)
Capture Length: 114 bytes (912 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:stun]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
```

Trang web 2: Bắt được 3720 gói tin

Tổng thời gian: 10.66s

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.

Dưới đây là 5 giao thức phổ biến mà bạn có thể thấy trong cột giao thức (Protocol) khi không áp dụng bộ lọc "http" khi truy cập hai website:

### 1. TCP (Transmission Control Protocol):

- **Chức năng:** TCP là giao thức truyền tải dữ liệu đáng tin cậy trong các mạng máy tính. Nó đảm bảo rằng dữ liệu được truyền đến đích mà không bị mất mát, thông qua việc phân mảnh và tổ chức lại các gói tin.

### 2. UDP (User Datagram Protocol):

- **Chức năng:** UDP là giao thức truyền tải không có kết nối, ít phức tạp hơn so với TCP. Nó không đảm bảo độ tin cậy trong việc truyền tải dữ liệu, nhưng có tốc độ nhanh hơn, thường được sử dụng trong các ứng dụng yêu cầu tốc độ như video streaming hoặc các cuộc gọi VoIP.

### 3. DNS (Domain Name System):



- **Chức năng:** DNS chuyển đổi tên miền (domain names) như "example.com" thành địa chỉ IP mà các máy tính có thể sử dụng để kết nối với nhau trong mạng Internet.

#### 4. ARP (Address Resolution Protocol):

- **Chức năng:** ARP được sử dụng để ánh xạ địa chỉ IP đến địa chỉ MAC (Media Access Control) trong một mạng nội bộ (LAN), giúp các thiết bị trong mạng xác định nhau.

#### 5. SSL/TLS (Secure Sockets Layer / Transport Layer Security):

- **Chức năng:** SSL và TLS là các giao thức mã hóa được sử dụng để bảo vệ sự riêng tư và tính toàn vẹn của dữ liệu trong quá trình truyền tải qua mạng, đặc biệt là trong các giao dịch qua HTTPS.

- 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).

Website 1:

- Thời gian gửi HTTP GET đầu tiên: 5.075462 giây
- Thời gian nhận HTTP 200 OK đầu tiên: 5.313100 giây
- Thời gian phản hồi:  $5.313100 - 5.075462 = 0.237638$  giây (238 ms)

No.	Time	Source	Destination	Protocol	Length	Info
1815	5.075462	192.168.1.5	125.234.100.252	HTTP	767	GET / HTTP/1.1
1893	5.313100	125.234.100.252	192.168.1.5	HTTP	883	HTTP/1.1 200 OK (text/html)
1973	5.487970	192.168.1.5	125.234.100.252	HTTP	718	GET /select2/ajax/get_settings HTTP/1.1
1988	5.510036	125.234.100.252	192.168.1.5	HTTP/1.1	66	HTTP/1.1 200 OK, JSON (application/json)

Website 2:

- Thời gian gửi HTTP GET đầu tiên: 114.239102 giây
- Thời gian nhận HTTP 200 OK đầu tiên: 114.496394 giây

Time	Source	Destination	Protocol	Length	Info
10863	114.239102	192.168.1.5	HTTP	654	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
19894	114.496394	128.119.245.12	HTTP	492	HTTP/1.1 200 OK (text/html)

- Thời gian phản hồi:  $114.496394 - 114.239102 = 0.257292$  giây (257 ms)

#### 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.

Có bắt được:

Trong tab Follow – HTTP Stream

```

Wireshark · Follow HTTP Stream (tcp.stream eq 68) · 1050070053-Bai1.pcapng

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
If-None-Match: "51-62f2db67e9f1c"
If-Modified-Since: Fri, 28 Feb 2025 06:14:02 GMT

HTTP/1.1 200 OK
Date: Fri, 28 Feb 2025 06:47:00 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Fri, 28 Feb 2025 06:46:01 GMT
ETag: "51-62f2e28e4dd9f"
Accept-Ranges: bytes
Content-Length: 81
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations! You've downloaded the first Wireshark lab file!
</html>
  
```

1 client pkt(s), 1 server pkt(s), 1 turn(s).

Entire conversation (1038 bytes)    Show as ASCII    No delta times    Stream 68

Find:    Case sensitive    Find Next

Filter Out This Stream    Print    Save as...    Back    Close    Help



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?

```
Command Prompt
Microsoft Windows [Version 10.0.26100.3194]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup gaia.cs.umass.edu
Server:  dns4.vietel.com.vn
Address:  203.113.131.2

Non-authoritative answer:
Name:     gaia.cs.umass.edu
Address:  128.119.245.12

C:\Users\Admin>
```

```
Command Prompt

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 9:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::d917:c046:b4a9:3660%21
IPv4 Address. . . . . : 192.168.98.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::b0fa:9fa7:5fec:b5f%18
IPv4 Address. . . . . : 192.168.198.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```



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.

#### **Diễn biến truy cập trang web**

1. Người dùng nhập URL vào trình duyệt.
2. Trình duyệt gửi yêu cầu DNS để phân giải tên miền thành địa chỉ IP.
3. Trình duyệt mở kết nối TCP với máy chủ thông qua giao thức HTTP/HTTPS.
4. Trình duyệt gửi yêu cầu HTTP GET đến máy chủ.
5. Máy chủ phản hồi với mã trạng thái HTTP (200 OK nếu thành công).
6. Trình duyệt tải xuống nội dung trang web và hiển thị cho người dùng.



Mở rộng: Theo bạn, địa chỉ IP dùng để làm gì và có cách nào khác để xem địa chỉ IP của máy tính và của một website khác hay không? Hãy thực hiện ví dụ minh họa.



