**A blue and orange background with dots and lines

Description automatically generated**

GVHD: **Phan Trung Phát**

Lớp: **IT005.O25.2**

|  |  |
| --- | --- |
| **Họ và tên** | **MSSV** |
| Vương Thành Đạt | 23520281 |

1

**Wireshark Getting Started**

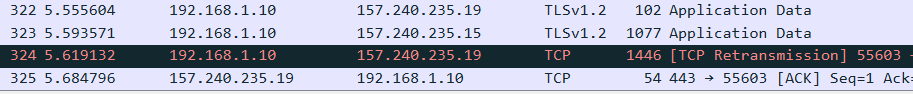
**ĐÁNH GIÁ KHÁC (\*):**

|  |  |
| --- | --- |
| **Nội dung** | **Kết quả** |
| Tổng thời gian thực hiện bài thực hành trung bình (1) | 10-15 phút/1 bài. |
| Link Video thực hiện (2)  *(nếu có)* |  |
| Ý kiến (3) *(nếu có)*  + Khó khăn  + Đề xuất … | Câu 13 khá khó trong việc nhận định protocol nào quan trọng. |
| Điểm tự đánh giá (4) | 8.5/10 |
| (\*): phần (1) và (4) bắt buộc thực hiện. | |

# Câu hỏi 1: Tổng thời gian bắt gói tin đối với website đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

## Minh chứng:

Nội dung: website http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html





Hình 1. Hình ảnh minh họa

## Giải thích:

* Tổng thời gian bắt gói tin với website trên là: 5.684796s
* Tổng số gói bắt được là 325

# Câu hỏi 2: Trong các gói tin bắt được, có tổng cộng bao nhiêu gói tin HTTP?

## Minh chứng:

Nội dung: gói http bắt được

A screenshot of a computer

Description automatically generated

## Giải thích:

* Có 4 gói tin HTTP trong Packet-display filter khi gõ “http”.

# Câu hỏi 3: 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 website. Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.

## Giải thích:

Nội dung.

1. **Giao thức TCP (Transmission Control Protocol)** là một trong các giao thức cốt lõi của bộ giao thức TCP/IP. Nó đảm bảo trao đổi thành công các gói dữ liệu giữa các thiết bị qua mạng bằng việc:

* Thiết lập và duy trì kết nói an toàn giữa các máy tính.
* Đảm bảo dữ liệu được truyền đi 1 cách tin cậy và đúng thứ tự.
* Xử lý lỗi và đảm bảo dữ liệu được nhận chính xác.

1. **Giao thức TLS (Transport Layer Security)** là một trong những giao thức quan trọng trong bộ giao thức TCP/IP. Nó được sử dụng để bảo mật việc truyền tải dữ liệu giữa các ứng dụng qua Internet:

* Bảo mật tầng vận chuyển; bảo vệ phiên truy cập trong trình duyệt web thông qua chuẩn HTTPS.
* Có thể dùng trong các phần mềm truyền tệp tin.
* Mã hóa thông tin và quan trọng thông tin liên lạc.

1. **Giao thức ARP (Address Resolution Protocol)** là một phần quan trọng của bộ giao thức TCP/IP. Nó được sử dụng để tìm ra địa chỉ phần cứng (địa chỉ MAC) của thiết bị từ một địa chỉ IP nguồn:

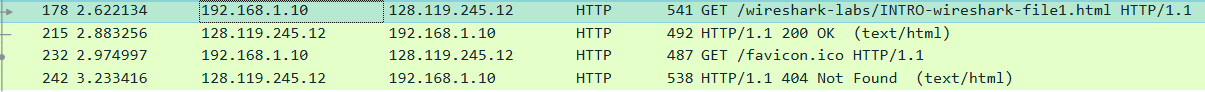
* Như một giao thức dịch địa chỉ chung cho các mạng IP.
* Cho phép mạng quản lý các kết nối độc lập với những thiết bị vật lý cụ thể được gắn vào từng mạng.

1. **UDP (User Datagram Protocol)** là một giao thức truyền tải dữ liệu nhanh và hiệu quả, không đảm bảo tính tin cậy và thứ tự. Nó thường được sử dụng cho các ứng dụng yêu cầu thời gian thực như streaming media, game trực tuyến và VoIP .
2. **Giao thức QUIC (Quick UDP Internet Connections)** là một giao thức truyền mạng được phát triển bởi Google từ năm 2012. QUIC sử dụng **UDP** thay vì **TCP** như các giao thức truyền tải thông thường. Nhờ đó QUIC có ưu điểm về tốc độ, hiệu suất và bảo mật trên Internet.

# Câu hỏi 4: Xác định gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm. Cho biết gói tin này cơ bản dùng để làm gì?

## Minh chứng:

Nội dung.

A screenshot of a computer

Description automatically generated

## Giải thích:

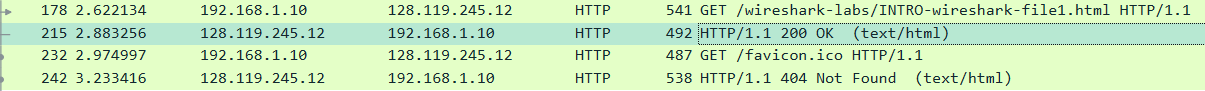
Nội dung.

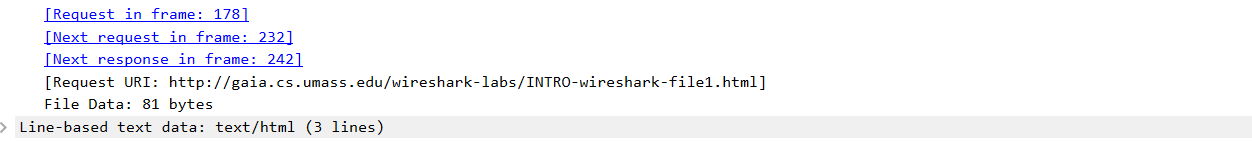
* Gói tin HTTP GET đầu tiên gửi đến website đã thử nghiệm là gói số 178.
* Ở phần packet details cho biết gói tin dùng để gửi request địa chỉ webiste, các thông tin user và phiên bản web đến server để truy cập, lấy thông tin về máy tính thông qua phương thức GET.

# Câu hỏi 5: Xác định gói tin phản hồi của gói tin HTTP GET ở câu 4, thông tin nào xác định điều đó?

## Minh chứng:

Nội dung.

A screen shot of a computer

Description automatically generated



## Giải thích:



Nội dung.

* Gói tin HTTP phản hồi đầu tiên của server là gói số 215.

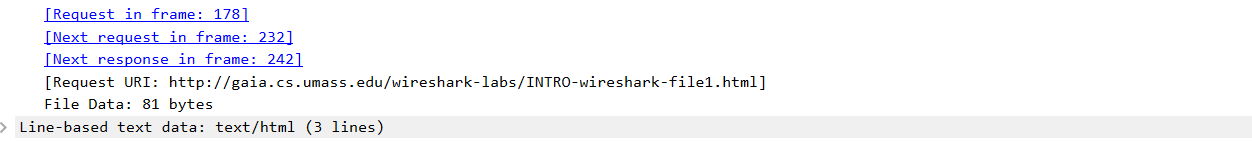


# Câu hỏi 6: Tính thời gian từ khi gói tin HTTP GET đầu tiên được gửi cho đến khi có gói tin phản hồi HTTP 200 OK đối với website đã thử nghiệm. (mặc định, giá trị của cột thời gian (Time) trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu bắt gói tin).

## Minh chứng:

Nội dung.

A screen shot of a computer

Description automatically generated



## Giải thích:

Nội dung.

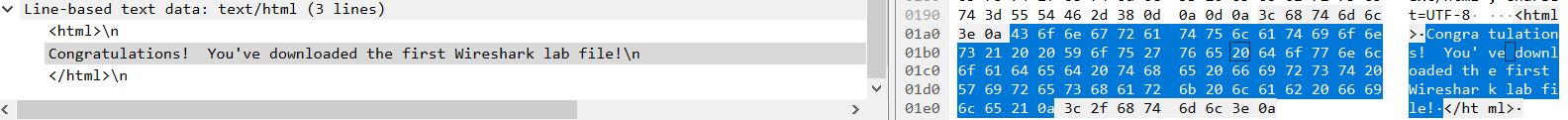
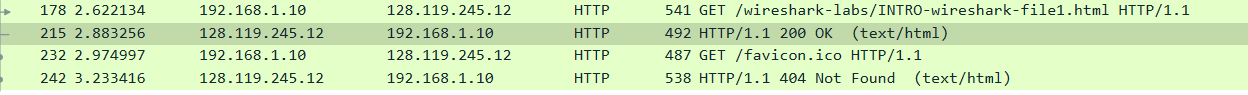
* Thời gian từ khi gửi đến khi nhận phản hồi là 0.261122000s



# Câu hỏi 7: 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.

## Minh chứng:

Nội dung.



## Giải thích:

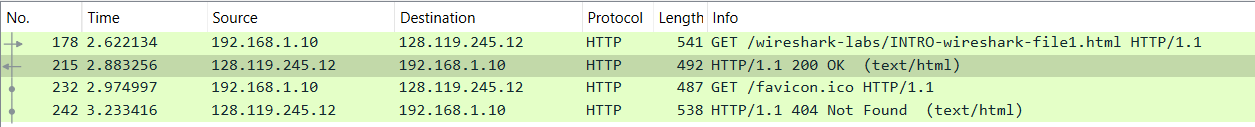
Nội dung.

* Nội dung hiển thị trên trang web có nằm trong gói HTTP/1.1 200 OK bắt được. Nằm ở mục Line-based text data trong phần packet details và packet draw.

# Câu hỏi 8: Hãy tìm hiểu về định dạng của địa chỉ IP và thử phỏng đoán địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính đang sử dụng là gì?

## Minh chứng:

Nội dung.

A black screen with white text

Description automatically generated

## Giải thích:

Nội dung.

* **Địa chỉ IP** là một chuỗi số được phân tách bằng dấu chấm. Địa chỉ IP được định dạng với **4 nhóm chữ số khác nhau**, mỗi nhóm có giá trị từ **0 đến 255. Có 5 địng dạng quan trọng:**

+ Địa chỉ IP công cộng: Dùng để xác định các thiết bị trên Internet.

+ Địa chỉ IP riêng tư: Dùng trong mạng nội bộ, không truy cập từ bên ngoài.

+ Địa chỉ IP tĩnh: Không thay đổi theo thời gian, được cấu hình thủ công.

+ Địa chỉ IP động: Thay đổi theo thời gian, được cấp tự động bởi DHCP.

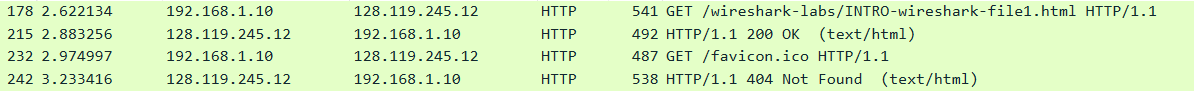
+ Địa chỉ IP loopback: Dùng để kiểm tra chức năng mạng trên chính thiết bị đó.

* Địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12 vì là Destination( điểm cuối từ máy tính đến server).
* Địa chỉ IP của máy tính đang sử dụng là 192.168.1.10 vì là Destination( điểm cuối từ server về máy tính).

# Câu hỏi 9: Từ các nội dung trên, hãy mô tả cơ bản khi truy cập một website (ví dụ website đã thử nghiệm ở trên) thì quá trình gửi và nhận gói tin đã hoạt động như thế nào? Trình duyệt mà bạn đang sử dụng đóng vai trò gì?

## Minh chứng:

Nội dung.



A screenshot of a computer

Description automatically generatedA screenshot of a computer code

Description automatically generated

## Giải thích:

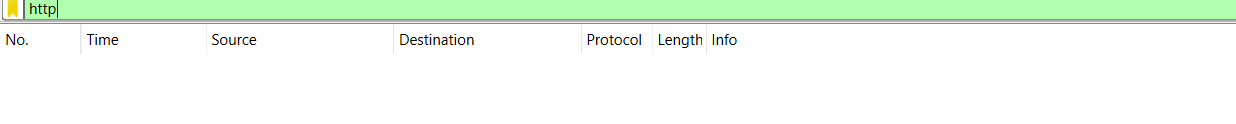
Nội dung.

* Khi truy cập 1 website, thì đầu tiên là máy tính sẽ gửi gói tin yêu cầu( HTTP GET) được cấp quyền truy cập từ máy đến địa chỉ IP của server-chứa URL(đường dẫn liên kết đến trang web)
* Sau đó server sẽ xác minh và xác nhận bằng việc gửi các gói tin phản hồi HTTP chứa mã trạng thái(200 OK), nội dung chứa dưới dạng(text/html/image).
* Trình duyệt nhận phản hồi HTTP và hiển thị nội dung của website, trình duyệt như ứng dụng giúp giao tiếp giữa web thông qua các protocol với các chức năng khác nhau để dễ dàng tiếp cận với user.

# Câu hỏi 10: Khi sử dụng bộ lọc “http” như ở đối với website ở Task 1 thì kết quả thu được như thế nào, có các gói tin HTTP tương tự không?

## Minh chứng:

Nội dung.



## Giải thích:

Nội dung.

* Khi dùng bộ lọc “http” như ở website Task 1, ta không thu được gói HTTP nào mà chỉ có các protocol khác.
* Các nguyên nhân:

+ **HTTPS và Mã hóa**: Hầu hết các trang web lớn sử dụng **HTTPS** thay vì **HTTP** để bảo mật dữ liệu. Khi ta truy cập một trang web qua HTTPS, dữ liệu được mã hóa và Wireshark không thể hiển thị nội dung bên trong gói tin.

+ **Cổng và Giao thức**: Một số trang web có thể sử dụng cổng không phải là cổng tiêu chuẩn của HTTP (cổng 80). Wireshark chỉ hiển thị gói tin HTTP nếu chúng sử dụng cổng 80 hoặc 443 (cho HTTPS).

+ **Bộ lọc và Cấu hình và Quyền truy cập.**

# Câu hỏi 11: Tìm cách xác định địa chỉ IP của website đã chọn là bao nhiêu? Địa chỉ IP của máy tính bạn lúc này là bao nhiêu?

## Minh chứng:

Nội dung.

A black screen with white text

Description automatically generatedA black screen with white text

Description automatically generated

## Giải thích:

Nội dung.

* Dùng terminal để xác định IP web qua “ping uit.edu.vn”: 118.69.123.140.
* Dùng terminal để xác định IP máy qua “ipconfig”: 192.168.1.10 mục wifi.

# Câu hỏi 12: Sử dụng thành phần packet-display filter để hiển thị đầy đủ quá trình trao đổi gói tin giữa máy tính của bạn và website bằng cú pháp: ip.addr== && ip.addr== . Cho biết rằng bạn có thể thấy được nội dung trả về của website không? Mô tả.

## Minh chứng:

Nội dung: Lọc ip. 118.69.123.140== && ip. 192.168.1.10

A screenshot of a computer

Description automatically generated

## Giải thích:

Nội dung.

* Không thấy nội dung trả về của website mà chỉ có 2 protocol chính: TCP và TLS, hai protocol có chức năng mã hóa dữ liệu giữa Client và Server, ngoại trừ các trường hợp có description key tương ứng với gói; TCP có chức năng thiết lập kết nối và truyền data.

# Câu hỏi 13: Hãy chỉ ra ít nhất 2 gói tin mà bạn cho rằng là quan trọng khi truy cập website này. Tìm hiểu và mô tả ngắn gọn các giao thức này. Giải thích.

## Minh chứng:

Nội dung.

1.

A white background with black text

Description automatically generated

## 2.



## A screenshot of a computer program Description automatically generated

## Giải thích:

Nội dung.

* Gói số 55, trong phần packet details, mục Handshake-SSL protocol có phần Key Share extension. Là gói tin khởi tạo liên kết từ máy khách đến máy chủ. Là loại bảo mật giúp mã hóa liên lạc giữa website và trình duyệt, sử dụng giao thức HTTPS để thiết lập kênh kết nối an toàn tới server thông qua tên miền mà khách truy cập.
* Gói số 61, trong phần packet details, có 2 mục TLS. Là gói tin liên quan đến bảo mật thông tin truyền giống như SSL, thông báo hoàn thành thiết lập bảo mật giữa máy khách và máy chủ. Gói tin cuối cùng chứa dữ liệu giao thức được truyền giữa 2 bên, đảm bảo tính bảo mật và truyền tin như đã nói.

# Câu hỏi 14: 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 thực hiện để minh họa điều đó. Tìm được càng nhiều cách càng tốt

## Minh chứng:

Nội dung: Các cách chủ yếu dò IP WiFi🡪Ipv4 address.

* Xem địa chỉ IP máy tính cá nhân:

1. Task Manager(ctrl+shift+esc)🡪 Performance🡪 WiFi🡪 Ipv4 address.

A screenshot of a computer

Description automatically generated

1. Terminal(window R+ cmd)🡪lệnh “ipconfig”🡪 WiFi🡪Ipv4 Address.

A screen shot of a computer

Description automatically generated

1. Window X+ settings🡪Network and Internet🡪Network and Sharing Center🡪 Connection WiFI🡪Details🡪Ipv4 Address

A screenshot of a computer

Description automatically generated

1. Window R + powershell**🡪 Get-NetIpAddress🡪WiFi🡪IDAddress.**

A screenshot of a computer program

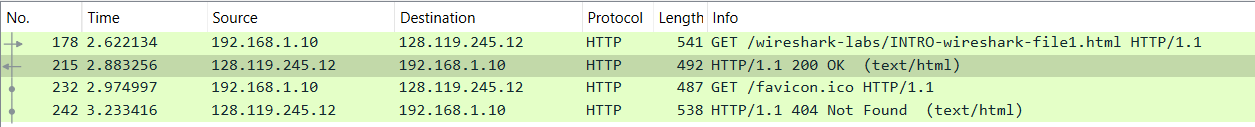
Description automatically generated

1. Icon WiFi thanh Taskbar🡪 Chọn vào WiFi đang dùng-mục Properties🡪Ipv4 Address.

A screenshot of a computer

Description automatically generated

1. Dùng WireShark cho biết điểm đầu và cuối giữa Client và Service.



* Xem địa chỉ IP website:

1. Terminal(window R+ cmd)🡪”ping”+tên website.

A black screen with white text

Description automatically generated

1. Terminal(window R+ cmd)🡪”tracert”+tên website.

A screenshot of a computer

Description automatically generated

1. Terminal(window R+ cmd)🡪”nslookup”+tên website.

A black background with white text

Description automatically generated

1. Dùng web (<https://checkip.com.vn/>) để kiểm tra.

A screenshot of a map

Description automatically generated

**HẾT**