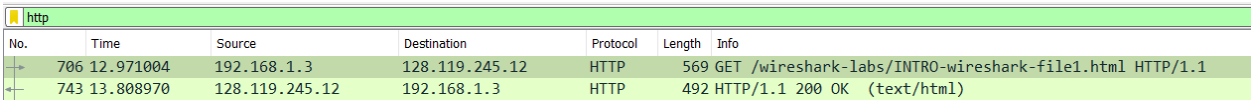
Câu 1:



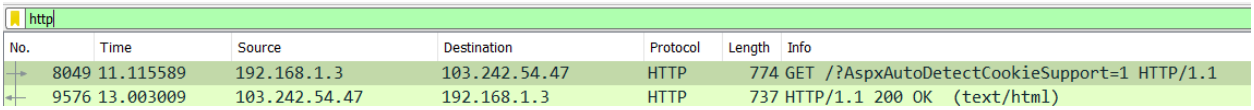
http

No.	Time	Source	Destination	Protocol	Length	Info
706	12.971004	192.168.1.3	128.119.245.12	HTTP	569	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
743	13.808970	128.119.245.12	192.168.1.3	HTTP	492	HTTP/1.1 200 OK (text/html)

Tổng thời gian bắt gói trang: 13.808970 – 12.971004 = 0.837966 (Giây)

Tổng số gói : 743 – 706 = 37 (Gói)

Trang web khác: http://online.gov.vn/



http

No.	Time	Source	Destination	Protocol	Length	Info
8049	11.115589	192.168.1.3	103.242.54.47	HTTP	774	GET /?AspxAutoDetectCookieSupport=1 HTTP/1.1
9576	13.003009	103.242.54.47	192.168.1.3	HTTP	737	HTTP/1.1 200 OK (text/html)

Tổng thời gian bắt gói trang: 13.003009 - 11.115589 = 1.88742 (Giây)

Tổng số gói : 9576 – 8049 = 1527 (Gói)

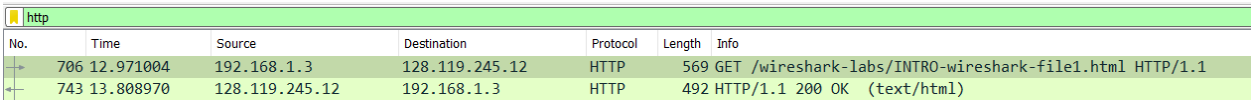
Câu 2:

5 giao thức khác nhau xuất hiện trong cột giao thức (Protocol) khi không áp dụng bộ lọc “http” khi truy cập 2 website:

1. **UDP** (***User Datagram Protocol***) 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.
2. **TCP** (*Transmission Control Protocol* - "Giao thức điều khiển truyền vận") là một trong các giao thức cốt lõi của bộ giao thức TCP/IP. Sử dụng TCP, các ứng dụng trên các máy chủ được nối mạng có thể tạo các "kết nối" với nhau, mà qua đó chúng có thể trao đổi dữ liệu hoặc các gói tin. Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự. TCP còn phân biệt giữa dữ liệu của nhiều ứng dụng (chẳng hạn, dịch vụ Web và dịch vụ thư điện tử) đồng thời chạy trên cùng một máy chủ.

3. **DNS** viết tắt của **Domain Name System** có nghĩa là hệ thống phân giải tên miền. DNS là hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên Internet.
4. **QUIC** là viết tắt của ***Quick Connections UDP Internet*** (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 (Transmission Control Protocol). QUIC chạy một dòng giao thức ghép kênh trên UDP (a multiplexed stream transport over UDP) thay vì TCP
5. **STUN** (Session Traversal Utilities for NAT) là một giao thức mạng cho phép các máy khách tìm ra địa chỉ công khai của mình, loại NAT mà chúng đang đứng sau và cổng phía Internet được NAT gắn liền với cổng nội bộ nào đó. Thông tin này được sử dụng để thiết lập giao tiếp UDP giữa 2 host mà đều nằm sau NAT router. Giao thức STUN được định nghĩa trong RFC 5389.

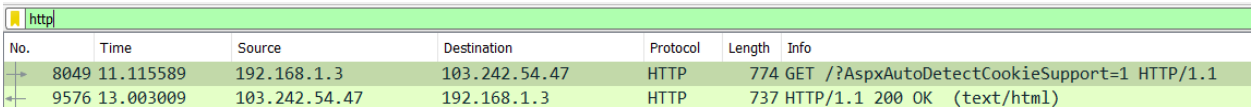
Câu 3:



Tổng thời gian bắt gói trang: 13.808970 – 12.971004 = 0.837966 (Giây)

Tổng số gói : 743 – 706 = 37 (Gói)

Trang web khác: http://online.gov.vn/

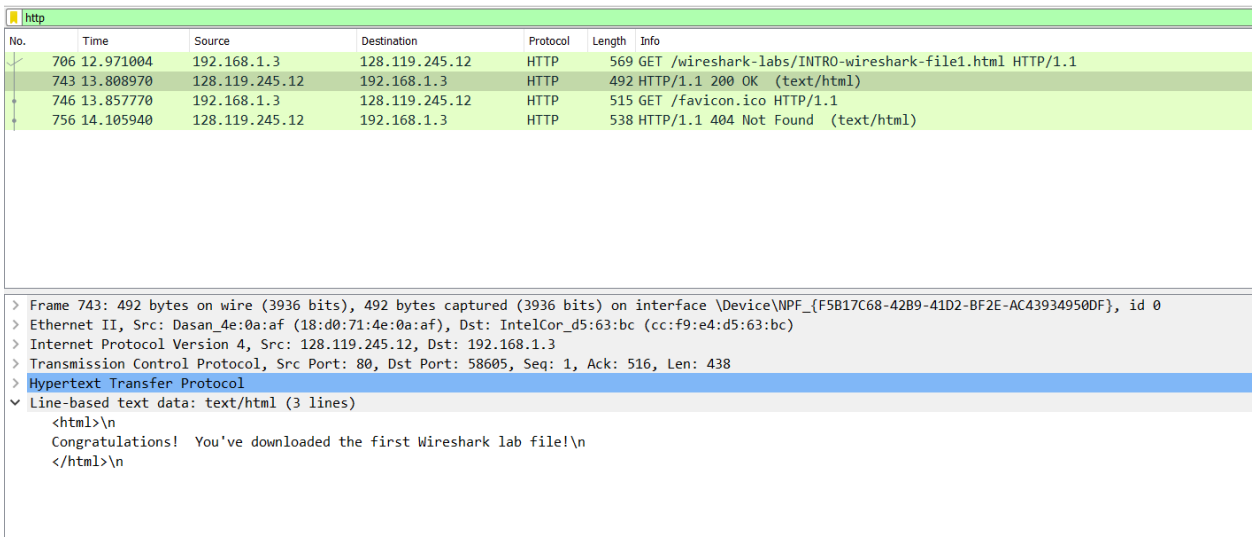


Tổng thời gian bắt gói trang: 13.003009 - 11.115589 = 1.88742 (Giây)

Tổng số gói : 9576 – 8049 = 1527 (Gói)

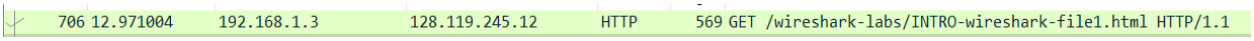
Câu 4:

- 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



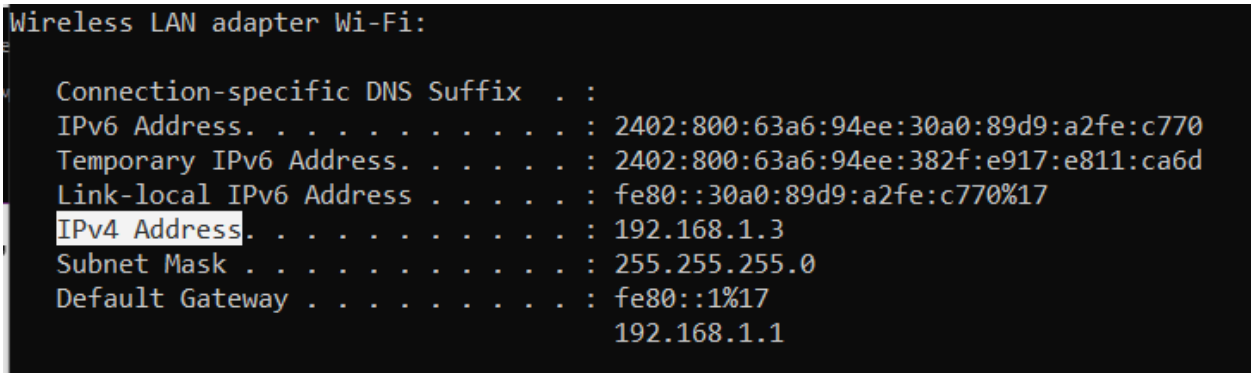
Câu 5:

Địa chỉ IP của gaia.cs.umass.edu: 128.119.245.12



Địa chỉ IP của website đã chọn: 103.242.54.47

Địa chỉ IP của máy tính : 192.168.1.3



Câu 6:

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:

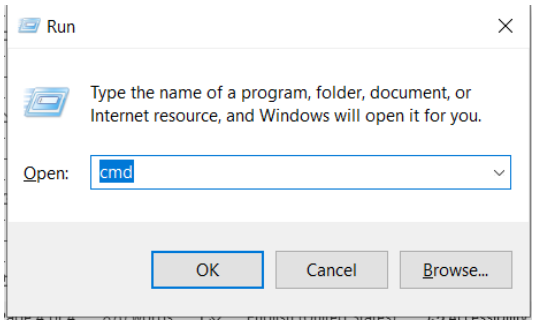
1. Khi truy cập trang web, trình duyệt sẽ gọi tới máy chủ DNS để biên dịch URL trang web thành một địa chỉ IP, mỗi trang web có địa chỉ IP riêng biệt. Khi tìm thấy địa chỉ IP của trang web chúng ta đang vào, địa chỉ IP đó sẽ được trả về cho trình duyệt.

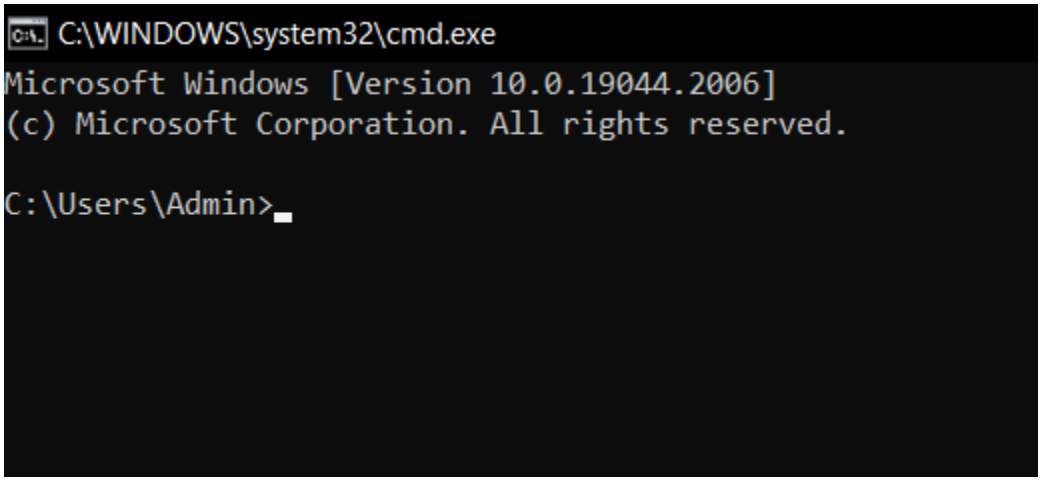
2. Trình duyệt sẽ sử dụng địa chỉ IP đó để yêu cầu HTTP gọi tới Server lưu trữ trang web đó. Nó sẽ kết nối cổng số 80 trên Server bằng giao thức TCP/IP.
3. Nếu Server chấp nhận thì sẽ gửi lại thông báo "200 OK". Và sau đó trình duyệt sẽ truy xuất mã HTML của trang web cụ thể được yêu cầu.
4. Khi trình duyệt của bạn nhận được mã HTML đó từ Server thì nó sẽ hiển thị ra cửa sổ của trình duyệt một trang web hoàn chỉnh - awesome!
5. Khi chúng ta đóng trình duyệt thì quá trình kết nối với Server sẽ kết thúc.

Mổ rộng:
Địa chỉ IP cung cấp danh tính của các thiết bị được kết nối mạng, giúp các thiết bị trên mạng internet phân biệt và nhận ra nhau, từ đó có thể giao tiếp với nhau.

Cách xem địa chỉ IP trên máy tính:

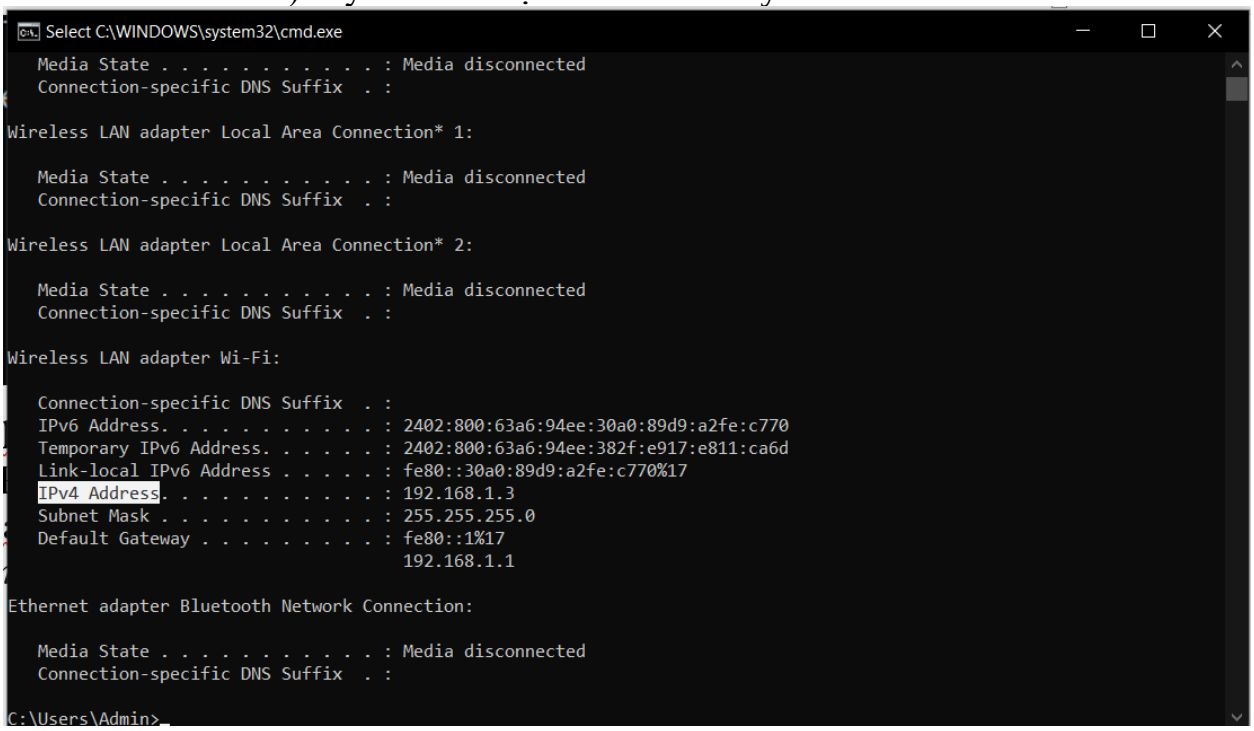
1. Mở CMD





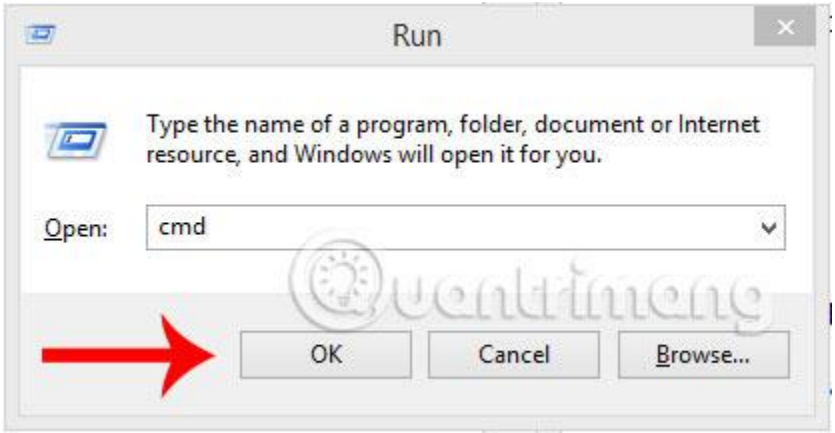
2. Nhập lệnh **ipconfig** > Enter

3. Tìm **IPv4 Address** hoặc **Link-local IPv6 Address** ở dưới tên kết nối (wifi là *Wireless LAN adapter Wi-Fi*, mạng dây là *Ethernet adapter Ethernet*) đây chính là địa chỉ IP của máy tính.

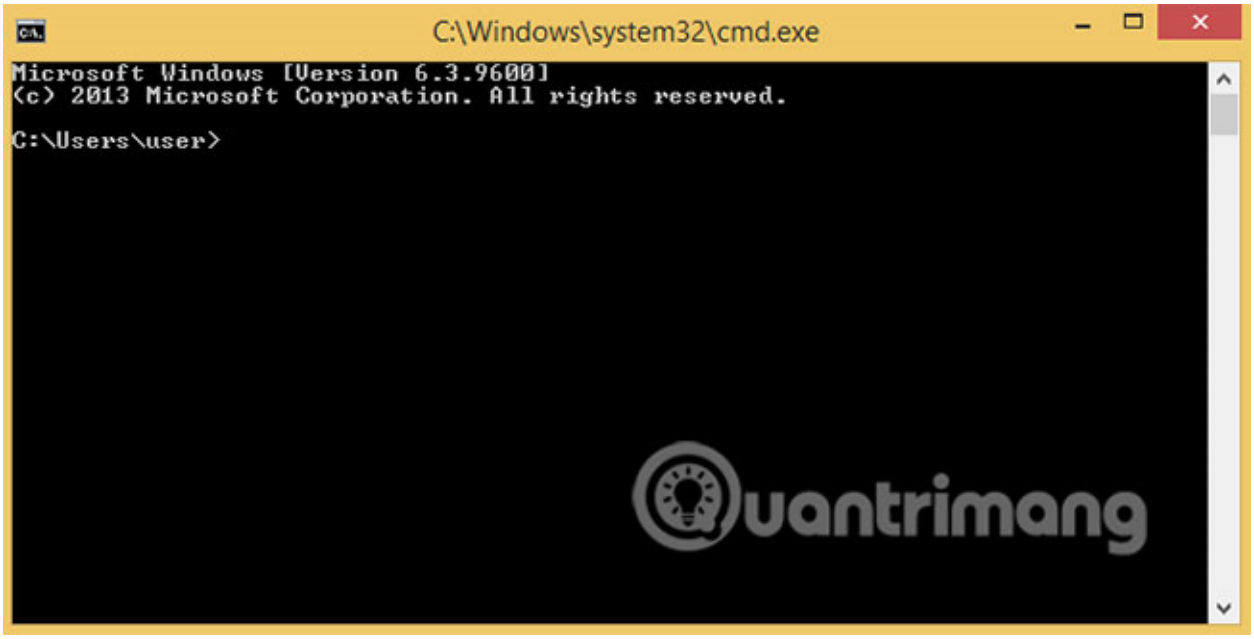


Cách xem địa chỉ Website:

Trên bàn phím máy tính, bạn nhấn tổ hợp phím **Windows + R** sau đó gõ lệnh **CMD** rồi nhấn **OK hoặc Enter** để truy cập vào Command Prompt.



Khi cửa sổ Command Prompt hiện ra, bạn gõ tên trang web bất kỳ với cú pháp **ping + tên miền muốn kiểm tra địa chỉ IP** rồi ấn **Enter** để xem địa chỉ IP trang web đó.



Chẳng hạn như trong hướng dẫn này, chúng ta thực hiện kiểm tra IP trang web http://online.gov.vn/thì sẽ nhập vào cửa sổ Command Prompt với nội dung ping http://online.gov.vn/ và nhấn Enter. Như bạn thấy, đây là kết quả địa chỉ IP của trang http://online.gov.vn/