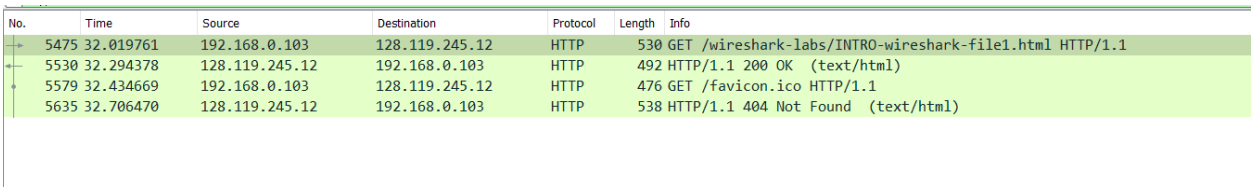
Câu 1: Tổng thời gian bắt gói tin trong từng trang web đã thử nghiệm và tổng số gói tin bắt được là bao nhiêu?

Trang web gaia.cs.umass.edu

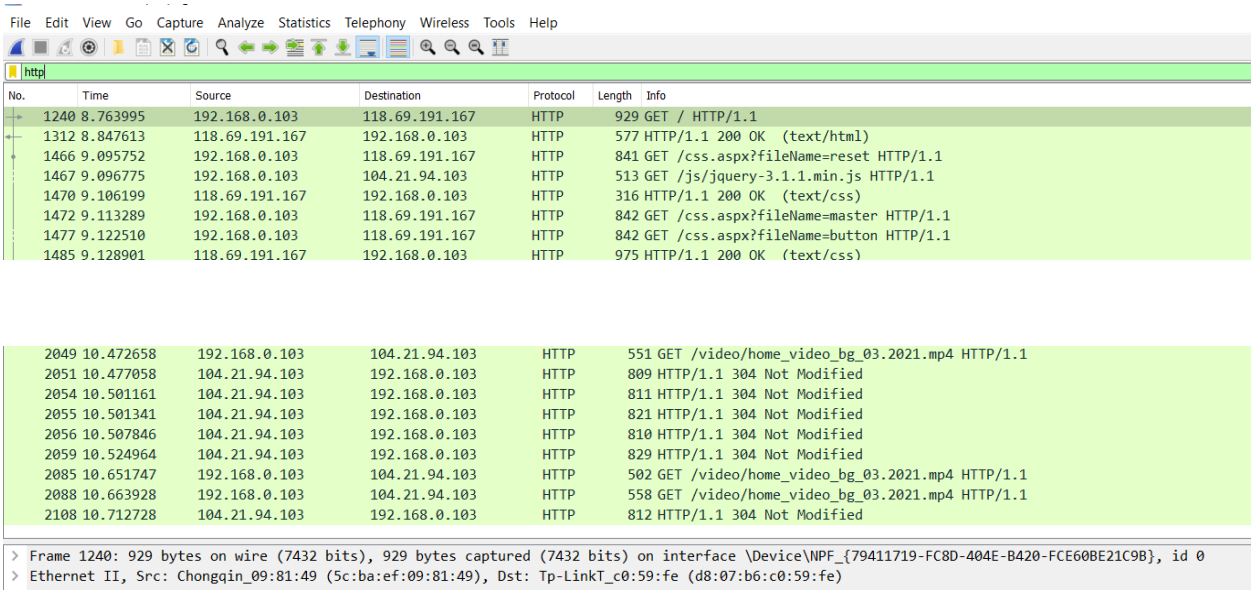


No.	Time	Source	Destination	Protocol	Length	Info
5475	32.019761	192.168.0.103	128.119.245.12	HTTP	530	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
5530	32.294378	128.119.245.12	192.168.0.103	HTTP	492	HTTP/1.1 200 OK (text/html)
5579	32.434669	192.168.0.103	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
5635	32.706470	128.119.245.12	192.168.0.103	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Tổng thời gian : 0.686709

Tổng gói tin : 5635

Trang web http://www.ttgdqp.edu.vn



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1240	8.763995	192.168.0.103	118.69.191.167	HTTP	929	GET / HTTP/1.1
1312	8.847613	118.69.191.167	192.168.0.103	HTTP	577	HTTP/1.1 200 OK (text/html)
1466	9.095752	192.168.0.103	118.69.191.167	HTTP	841	GET /css.aspx?fileName=reset HTTP/1.1
1467	9.096775	192.168.0.103	104.21.94.103	HTTP	513	GET /js/jquery-3.1.1.min.js HTTP/1.1
1470	9.106199	118.69.191.167	192.168.0.103	HTTP	316	HTTP/1.1 200 OK (text/css)
1472	9.113289	192.168.0.103	118.69.191.167	HTTP	842	GET /css.aspx?fileName=master HTTP/1.1
1477	9.122510	192.168.0.103	118.69.191.167	HTTP	842	GET /css.aspx?fileName=button HTTP/1.1
1485	9.128901	118.69.191.167	192.168.0.103	HTTP	975	HTTP/1.1 200 OK (text/css)

2049	10.472658	192.168.0.103	104.21.94.103	HTTP	551	GET /video/home_video_bg_03.2021.mp4 HTTP/1.1
2051	10.477058	104.21.94.103	192.168.0.103	HTTP	809	HTTP/1.1 304 Not Modified
2054	10.501161	104.21.94.103	192.168.0.103	HTTP	811	HTTP/1.1 304 Not Modified
2055	10.501341	104.21.94.103	192.168.0.103	HTTP	821	HTTP/1.1 304 Not Modified
2056	10.507846	104.21.94.103	192.168.0.103	HTTP	810	HTTP/1.1 304 Not Modified
2059	10.524964	104.21.94.103	192.168.0.103	HTTP	829	HTTP/1.1 304 Not Modified
2085	10.651747	192.168.0.103	104.21.94.103	HTTP	502	GET /video/home_video_bg_03.2021.mp4 HTTP/1.1
2088	10.663928	192.168.0.103	104.21.94.103	HTTP	558	GET /video/home_video_bg_03.2021.mp4 HTTP/1.1
2108	10.712728	104.21.94.103	192.168.0.103	HTTP	812	HTTP/1.1 304 Not Modified

> Frame 1240: 929 bytes on wire (7432 bits), 929 bytes captured (7432 bits) on interface \Device\NPF_{79411719-FC8D-404E-B420-FCE60BE21C9B}, id 0
> Ethernet II, Src: Chongqin_09:81:49 (5c:ba:ef:09:81:49), Dst: Tp-LinkT_c0:59:fe (d8:07:b6:c0:59:fe)

Tổng thời gian:1,948733

Tổng gói tin: 2108

Câu 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.

TCP : Giao thức này đảm bảo chuyển giao dữ liệu tới nơi nhận một cách đáng tin cậy và đúng thứ tự.

UDP : UDP được sử dụng để gửi các gói tin ngắn gọi là datagram, cho phép truyền nhanh hơn,

được sử dụng khi tốc độ được ưu tiên và sửa lỗi không cần thiết.

DNS : là một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền trên internet. Nhờ giao thức này nên có thể chuyển đổi tên miền thành địa chỉ IP.

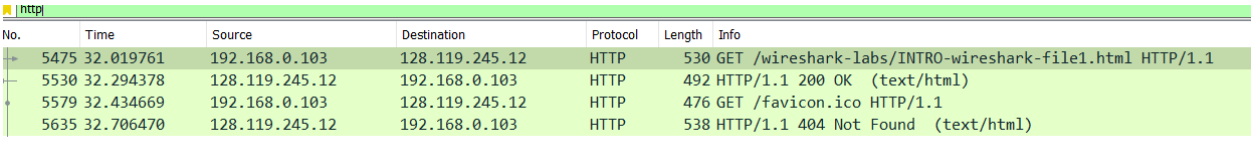
HTTP : Giao thức này dùng để liên hệ thông tin giữa máy cung cấp dịch vụ (Web server) và Máy sử dụng dịch vụ (Web client).

STUN : 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.

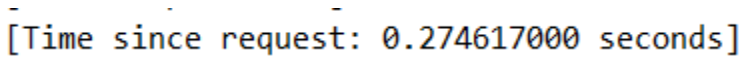
Nguồn : https://ictsaigon.vn/14-giao-thuc-mang-pho-bien-dang-su-dung-hien-nay/

Câu 3: 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).

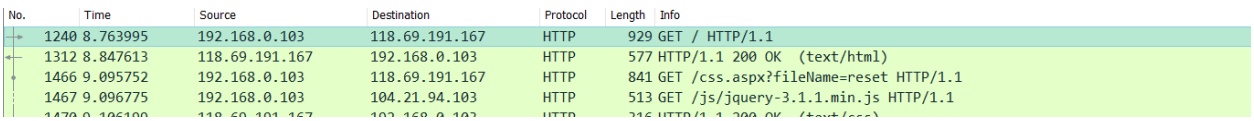
Trang web gaia.cs.umass.edu



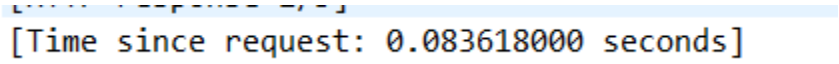
No.	Time	Source	Destination	Protocol	Length	Info
5475	32.019761	192.168.0.103	128.119.245.12	HTTP	530	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
5530	32.294378	128.119.245.12	192.168.0.103	HTTP	492	HTTP/1.1 200 OK (text/html)
5579	32.434669	192.168.0.103	128.119.245.12	HTTP	476	GET /favicon.ico HTTP/1.1
5635	32.706470	128.119.245.12	192.168.0.103	HTTP	538	HTTP/1.1 404 Not Found (text/html)



Trang web http://www.ttgdqp.edu.vn

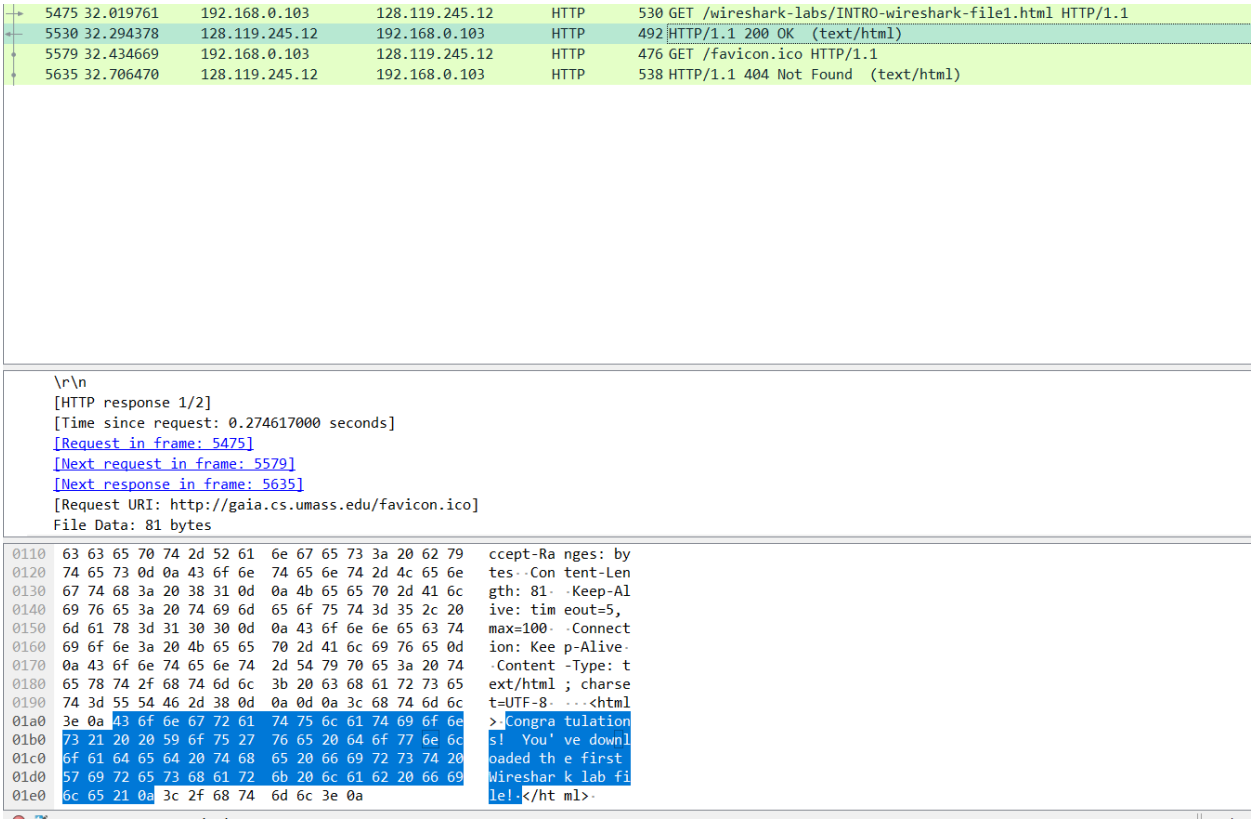


No.	Time	Source	Destination	Protocol	Length	Info
1240	8.763995	192.168.0.103	118.69.191.167	HTTP	929	GET / HTTP/1.1
1312	8.847613	118.69.191.167	192.168.0.103	HTTP	577	HTTP/1.1 200 OK (text/html)
1466	9.095752	192.168.0.103	118.69.191.167	HTTP	841	GET /css.aspx?fileName=reset HTTP/1.1
1467	9.096775	192.168.0.103	104.21.94.103	HTTP	513	GET /js/jquery-3.1.1.min.js HTTP/1.1



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 hay không? Nếu có, hãy tìm và xác định vị trí của nội dung này trong các gói tin bắt được

Có hiển thị trong gói tinh thứ 2



Câu 5:

IP gaia.cs.umass.edu : 128.119.245.12

IP ttgdqp.edu.vn : 118.69.191.167

IP máy : 192.168.0.103

Câu 6 :

Khi trình duyệt đầu tiên sẽ tìm địa chỉ web đó qua giao thức DNS và sẽ gửi yêu cầu HTTP tới trang web đó, sau đó web sẽ lại gửi phản hồi đến máy tính và sẽ chạy nội dung trang web đó.

Câu thêm :

địa chỉ IP(Internet Protocol) có nghĩa là địa chỉ giao thức của internet, nó tương tự như địa chỉ nhà hay địa chỉ. Các thiết bị phần cứng trong mạng muốn kết nối và giao tiếp với nhau được đều phải có địa chỉ IP.

Có thể xem IP bằng terminal hoặc command promt .

Ví dụ