

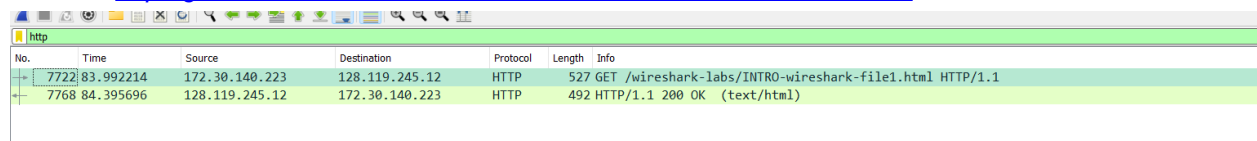
Tên: Nguyễn Thành Đăng
MSSV: 21520683
Mã lớp: IT005.N12

LAB01: WIRESHARK

Task 1:

- Một số thiết bị liên quan đến mạng: Điện thoại, laptop, router, TV,...
- Vấn đề xảy ra nếu không có Internet trong 5 phút: Sẽ không có các giao dịch quốc tế, dây chuyền tự động không thể làm việc dẫn đến nhiều vấn đề trong sản xuất,...
- Mục tiêu khi học nhập môn mạng máy tính: Nắm được cơ chế hoạt động của đường truyền mạng, quản lý được các thiết bị kết nối mạng. Đặc biệt là vững nền tảng kiến thức cho các môn chuyên ngành.

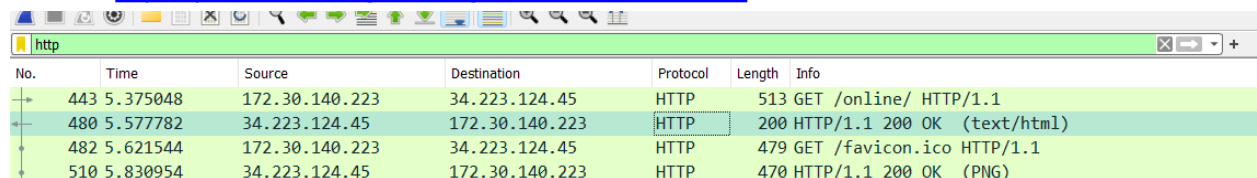
Website: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>



The screenshot shows a Wireshark packet capture for an HTTP session. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
7722	83.992214	172.30.140.223	128.119.245.12	HTTP	527	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
7768	84.395696	128.119.245.12	172.30.140.223	HTTP	492	HTTP/1.1 200 OK (text/html)

Website: <http://splendidserenegrandlaugh.neverssl.com/online/>



The screenshot shows a Wireshark packet capture for an HTTP session. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
443	5.375048	172.30.140.223	34.223.124.45	HTTP	513	GET /online/ HTTP/1.1
480	5.577782	34.223.124.45	172.30.140.223	HTTP	200	HTTP/1.1 200 OK (text/html)
482	5.621544	172.30.140.223	34.223.124.45	HTTP	479	GET /favicon.ico HTTP/1.1
510	5.830954	34.223.124.45	172.30.140.223	HTTP	470	HTTP/1.1 200 OK (PNG)

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?

Website 1:

- Tổng thời gian bắt gói tin: 84.395696 (s)
- Tổng số gói tin bắt được: 7768 (gói)

Website 2:

- Tổng thời gian bắt gói tin: 5.577782 (s)
- Tổng số gói tin bắt được: 480 (gói)

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.

Các giao thức xuất hiện: TCP, SSDP, MDNS, UDP, ARP,...

- 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.

- SSDP: (*Simple Service Discovery Protocol* - “Giao thức khám phá dịch vụ đơn giản”) là tiêu chuẩn cho các dịch vụ quảng cáo trên mạng TCP/IP và phát hiện ra chúng. Giao thức Universal Plug and Play (UPnP) sử dụng SSDP để thông báo và tìm thiết bị theo thứ tự, chẳng hạn như để truyền video từ nguồn đến hệ thống phát lại.
- MDNS: (*Multicast Domain Name System* - “DSN đa phương tiện”) là giao thức để liên kết một tên máy chủ với một địa chỉ IP mà không cần sử dụng DNS. Chọn hộp kiểm tra để kích hoạt mDNS và nhập tên mDNS vào hộp văn bản [mDNS Name].
- UDP: (*User Datagram Protocol* - “Giao thức dữ liệu người dùng”) 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.
- ARP: (*Address Resolution Protocol* - “Giao thức mạng”) là một giao thức truyền thông được sử dụng để chuyển địa chỉ từ tầng mạng (Internet layer) sang tầng liên kết dữ liệu theo mô hình OSI.

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).

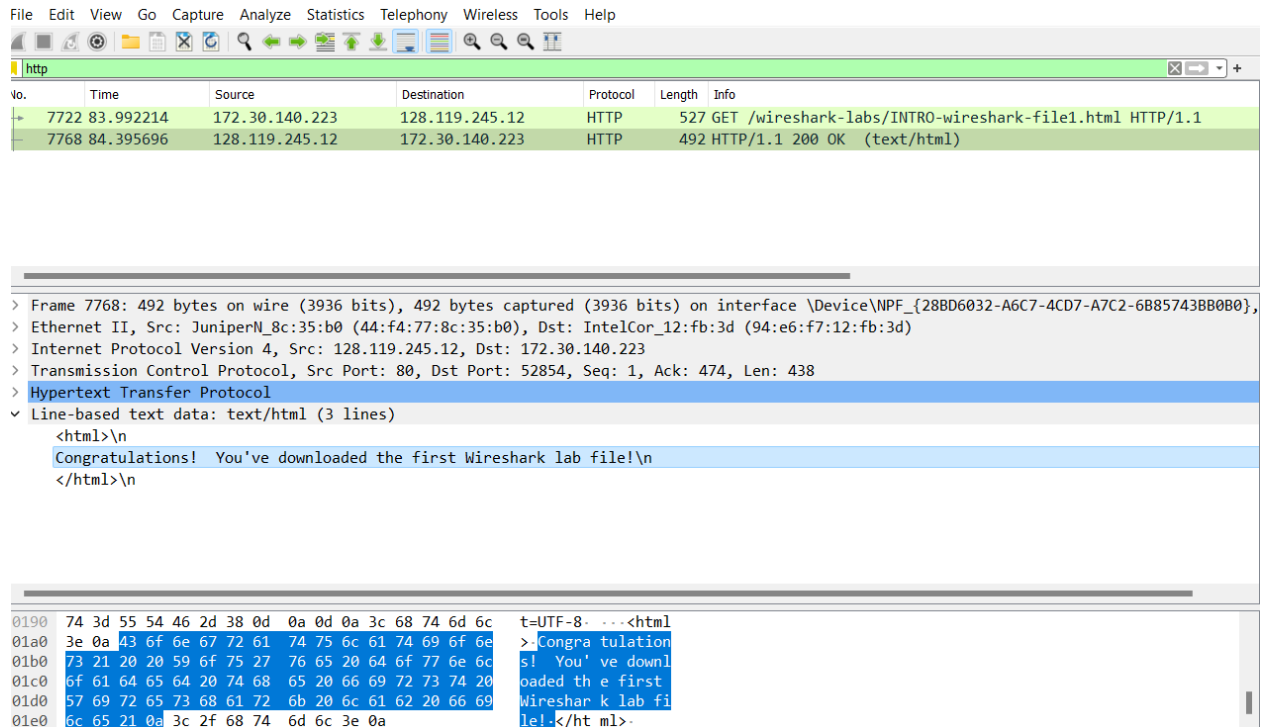
Website 1:

- Tổng thời gian bắt gói tin: 0.403149 (s)

Website 2:

- Tổng thời gian bắt gói tin: 0.202734 (s)

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. Nội dung này **CÓ** nằm trong gói tin bắt được.



Nằm trong gói 7768.

Câu 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?

Địa chỉ IP của website 1: 128.119.245.12

Địa chỉ IP của website 2: 34.223.124.45

Địa chỉ IP của máy tính sử dụng: 172.30.140.223

Câu 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.

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. Trình duyệt sẽ sử dụng địa chỉ IP đó để yêu cầu HTTP gọi tới Server lưu trữ trang web đó. 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. 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. Khi đóng trình duyệt thì quá trình kết nối với Server sẽ kết thúc.