

**BÀI TẬP THỰC HÀNH SỐ 1**

**MÔN HỌC: NHẬP MÔN MẠNG MÁY TÍNH**

|  |
| --- |
|  |

# GIỚI THIỆU WIRESHARK

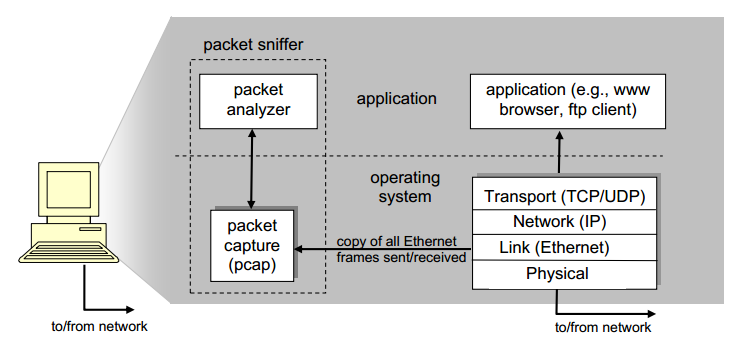
# Lời mở đầu

Các giao thức mạng có thể được hiểu sâu hơn bằng cách quan sát chuỗi các thông điệp trao đổi giữa hai máy tính, nghiên cứu sâu các hành động của giao thức trong những trường hợp cụ thể. Điều này có thể đạt được bằng cách thực hiện các kịch bản mô phỏng trong môi trường mạng thực tế như Internet. Trong các bài thực hành Wireshark, chúng ta sẽ chạy nhiều ứng dụng mạng trong các kịch bản khác nhau sử dụng máy tính cá nhân trên môi trường mạng Internet.

Trong bài thực hành đầu tiên, chúng ta sẽ làm quen với Wireshark và thực hiện bắt các gói tin cơ bản, sau đó quan sát chúng.

Công cụ để quan sát các thông điệp trao đổi giữa các máy tính được gọi là công cụ bắt trộm gói tin(**packet sniffer**). Các công cụ này bắt trộm các gói tin được gửi đi hoặc nhận về máy tính. Chúng hoạt động ẩn bên dưới và không gửi bất kỳ gói tin nào. Các gói tin bị bắt trộm chỉ là bản sao chép của gói tin chính.

Hình 1 cho thấy cấu trúc của công cụ bắt trộm gói tin. Bên phải hình 1 là các giao thức (các giao thức trên Internet) và các ứng dụng (như là web browser và ftp client) chạy trên máy tính của bạn. Công cụ bắt trộm gói tin được thể hiện trong hình chữ nhật nét đứt là một phần mềm trên máy tính gồm có 2 phần. **Thư viện bắt gói tin** nhận bản sao của mỗi frame trên tầng liên kết dữ liệu được gửi đi hoặc nhận về máy tính. Nhắc lại rằng các thông điệp được trao đổi bởi các giao thức tầng cao hơn như HTTP, FTP, TCP, UDP, DNS hoặc IP đều được đóng gói trong frame ở tầng liên kết dữ liệu. Trong hình, môi trường truyền dẫn vật lý được giả định là Ethernet nên các gói tin ở các giao thức tầng trên đều được đóng gói trong Ethernet frame. Việc bắt các frames giúp chúng ta quan sát tất cả các thông điệp được gửi đi và nhận về máy tính của mình.



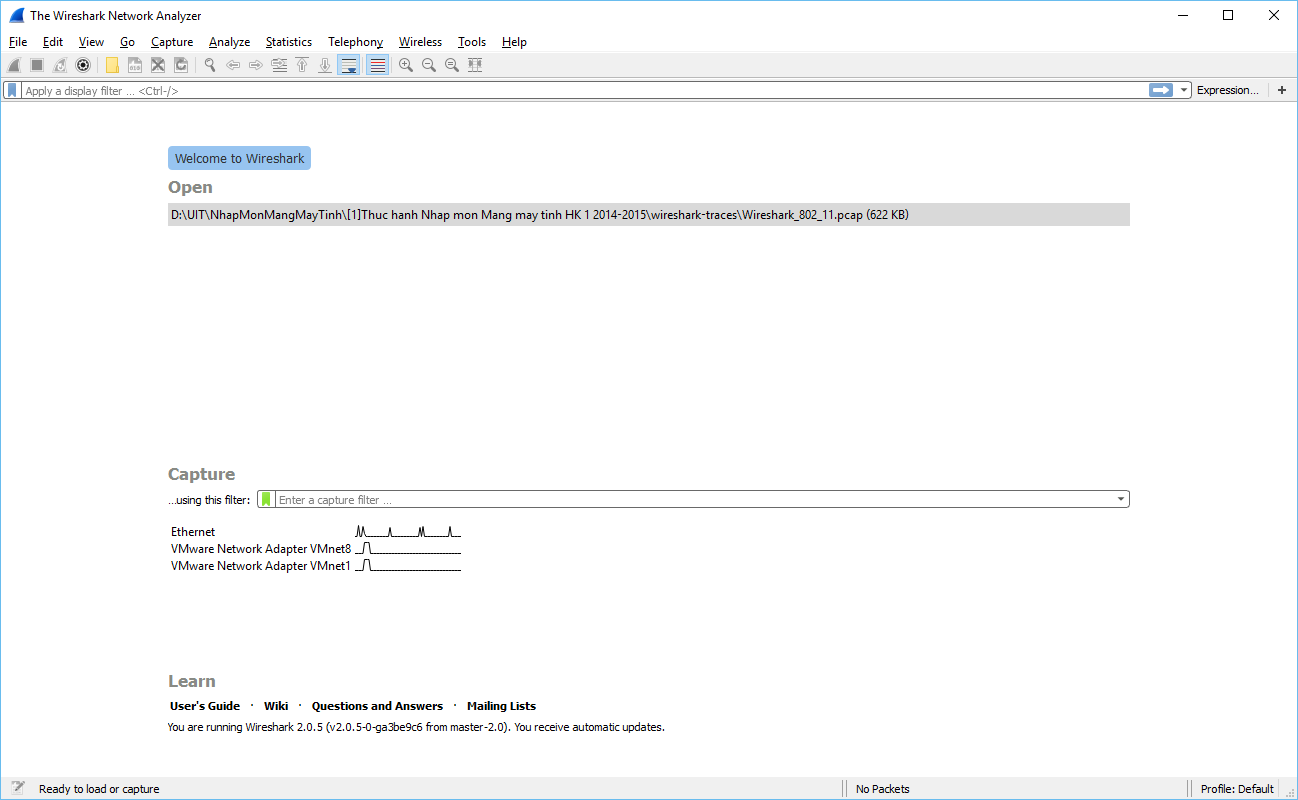
***Hình 1: Cấu trúc của công cụ bắt trộm gói tin***

Thành phần thứ 2 của một công cụ bắt trộm gói tin chính là **bộ phân tích gói**. Bộ phân tích gói có nhiệm vụ hiển thị nội dung của các trường trong một gói tin. Để làm được điều đó, bộ phân tích gói phải hiểu cấu trúc của tất cả các gói tin được trao đổi bởi các giao thức. Ví dụ, giả sử chúng ta quan tâm đến nội dung các trường trong các thông điệp của giao thức HTTP. Bộ phân tích gói phải hiểu định dạng của Ethernet frames, IP datagram, TCP segment và cuối cùng rút trích nội dung của thông điệp HTTP chứa trong TCP segment. Ngoài ra, bộ phân tích gói cũng hiểu giao thức HTTP và biết được các bytes đầu tiên trong thông điệp HTTP chứa chuỗi “GET”, “POST” hoặc “HEAD”.

Chúng ta sẽ sử dụng công cụ Wireshark [<http://www.wireshark.org/>] cho các bài thực hành. Nó cho phép bạn quan sát nội dung của các thông điệp được trao đổi bởi các giao thức tại các tầng khác nhau. Wireshark là một công cụ phân tích giao thức mạng miễn phí chạy trên Windows, Linux/Unix và Mac. Bạn có thể tìm đọc thêm các hướng dẫn về Wireshark tại địa chỉ:  
 [http://www.wireshark.org/docs/wsug\_html\_chunked/](http://www.wireshark.org/docs/wsug_html_chunked/))   
hoặc [http://www.wireshark.org/docs/man-pages/   
và các câu hỏi thường gặp tại](http://www.wireshark.org/docs/man-pages/%20và%20các%20câu%20hỏi%20thường%20gặp%20tại%20%20) <http://www.wireshark.org/faq.html>

Để chạy Wireshark, bạn phải cài Wireshark và thư viện bắt gói tin *libpcap* hoặc *winPCap*. Nếu thư viện *winPCap* chưa có trên máy tính, nó sẽ được cài trong quá trình cài Wireshark. Địa chỉ download: <http://www.wireshark.org/download.html>

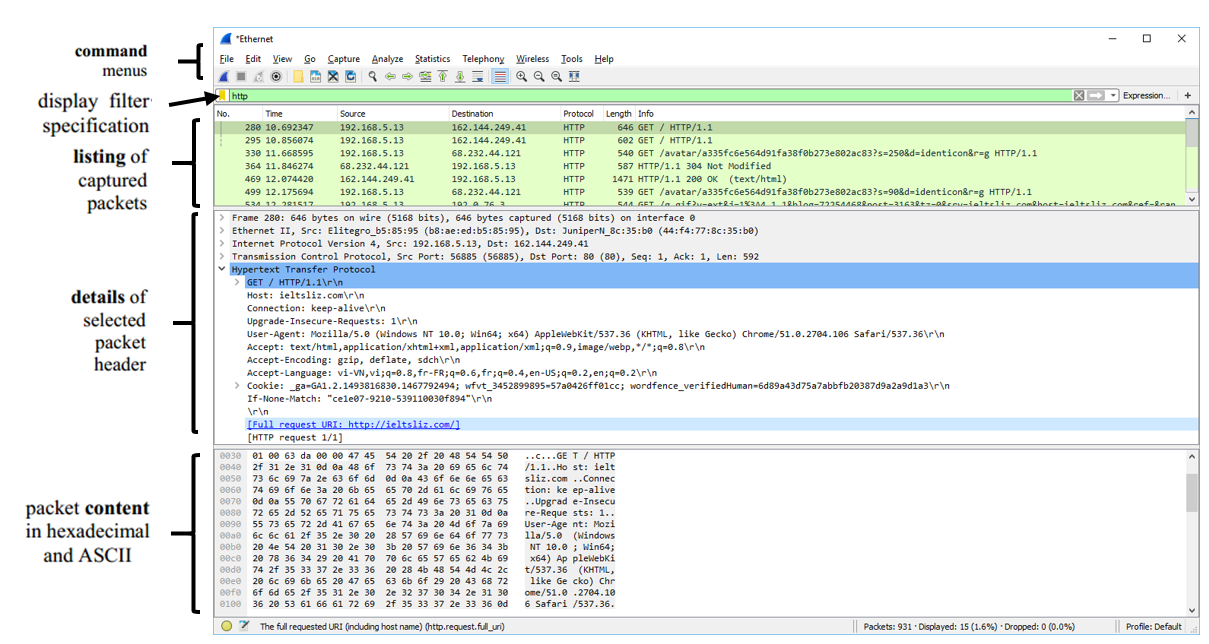
Khi khởi động Wireshark, bạn sẽ thấy giao diện sau:



***Hình 2: Giao diện khởi động Wireshark (v2.0.5)***

Nhìn vào góc giữa của giao diện, bạn sẽ thấy “Interface list”. Đây là danh sách của các network interfaces trên máy tính. Sau khi chọn một interface, Wireshark sẽ bắt tất cả các gói tin đi qua interface đó. Trong ví dụ ở trên, có một Ethernet interface và một hai VMware interface

Nếu click vào một trong những interfaces đó để bắt đầu bắt gói tin, một màn hình hiện ra như bên dưới, hiển thị thông tin về các gói tin bị bắt. Sau khi đã bắt gói tin, bạn có thể dừng lại bằng cách chọn Stop trên thanh menu.



***Hình 3: Giao diện chính của Wireshark trong suốt quá trình bắt và phân tích gói tin***

Giao diện Wireshark gồm có 5 thành phần chính:

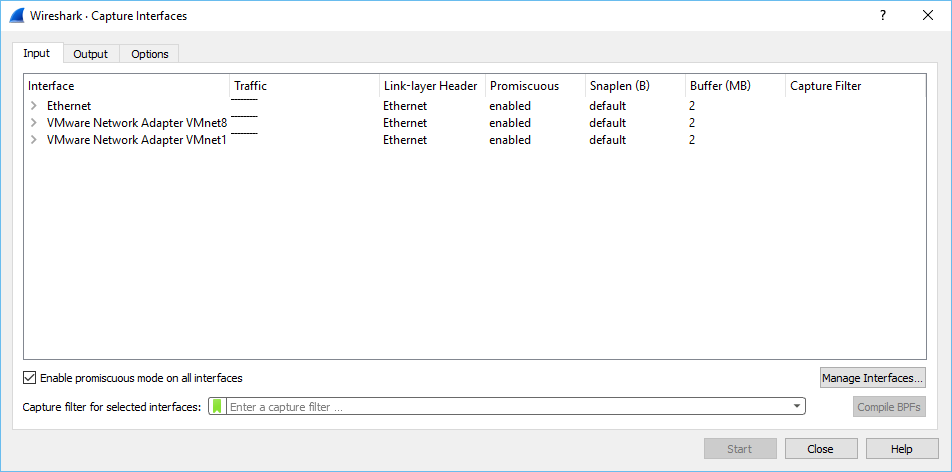
* **Command menus**: chứa các menu thực hiện các chứng năng chính của Wireshark. Chúng ta quan tâm đến File và Capture. File menu cho phép lưu các gói tin đã bị bắt hoặc mở file chứa các gói tin đã bắt từ trước. Capture menu cho phép bắt đầu bắt gói tin.
* **Packet-listing windows**: hiển thị dòng thông tin tóm tắt cho từng gói tin bị bắt, bao gồm số thứ tự (số này được gán bởi Wireshark, không phải số thứ tự chứa trong header của gói tin), thời gian gói tin bị bắt, địa chỉ nguồn và đích, loại giao thức và thông tin đặc tả cho giao thức đó. Bạn có thể sắp xếp các dòng theo các tiêu chí bằng cách nhấp vào tên các cột tương ứng. Cột Protocol hiển thị giao thức hoạt động ở tầng cao nhất.
* **Packet-header details window**: cung cấp các thông tin chi tiết về gói tin được chọn từ packet-listing window. 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. Cuối cùng, thông tin về giao thức ở tầng cao nhất cũng được hiển thị.
* **Packet-contents window** hiển thị toàn bộ nội dung của frame dưới dạng ASCII và hexadecimal.
* Hướng lên trên của giao diện Wireshark là **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, chúng ta sử dụng packet-display filter để Wireshark ẩn tất cả các gói tin bắt được ngoại trừ những gói tin tương ứng với HTTP bằng cách gõ “http” vào khung này và chọn Apply.

# Thử nghiệm Wireshark

Ghi chú rằng nếu bạn không thể chạy Wireshark trên Internet thật sự thì có thể mở file Wireshark\_intro có sẵn trong thư mục wireshark-traces.

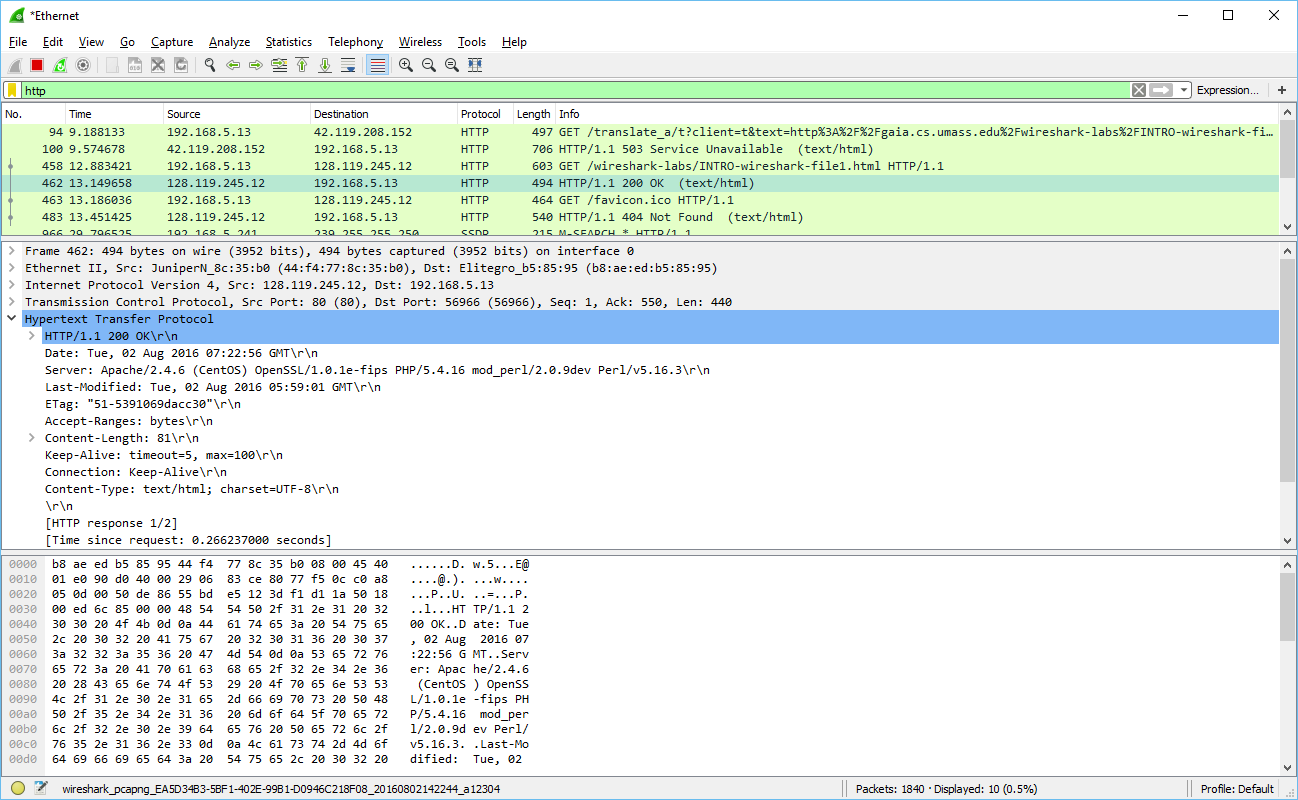
Giả định rằng máy tính bạn có kết nối Internet. Thực hiện các bước sau

* Khởi động Web browser.
* Khởi động phần mềm Wireshark.
* Chọn Capture và chọn Interfaces.



***Hình 4: Wireshark Capture Interface Window***

* Chọn Start đối với interface mà bạn muốn bắt gói tin. Lúc này Wireshark bắt đầu bắt tất cả các gói tin được gửi đến hoặc nhận về máy tính.
* Sau khi đã bắt đầu bắt gói tin, một cửa sổ hiện ra như trong hình 3. Cửa sổ này hiển thị các packet đang được bắt. Chọn menu Capture và sau đó chọn Stop khi bạn muốn dừng bắt gói tin. Tuy nhiên, đừng dừng bắt lúc này vì bạn nên thử với một kết nối HTTP.
* Trong khi Wireshark đang hoạt động, trên web browser, gõ: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html> và website sẽ hiện ra trên trình duyệt. Lúc này các Ethernet frames chứa các thông điệp HTTP đã được bắt bởi Wireshark.
* Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là một dòng chào mừng đơn giản), dừng bắt gói tin. Cửa sổ chính của Wireshark bây giờ giống như hình 3. Bạn đã có các gói tin chứa đầy đủ các thông điệp được trao đổi giữa máy tính và web server. Thông điệp HTTP trao đổi với gaia.cs.umass.edu web server phải xuất hiện đâu đó trong các gói tin được bắt. Có nhiều loại gói tin được hiển thị (tương ứng với nhiều giao thức). Mặc dù bạn chỉ đơn thuần download một trang web nhưng có nhiều giao thức khác chạy bên dưới mà bạn không thấy được.
* Gõ “http” (không có ngoặc kép) vào packet-display filter sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window.
* Tìm thông điêp 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). Sau khi chọn thông điệp HTTP GET, Ethernet frame, IP datagram, TCP segment và HTTP header sẽ được hiển thị ở packet-header window.
* Thoát Wireshark



***Hình 5: Cửa sổ Wireshark sau bước 9***

Trả lời các câu hỏi sau đây:

1. Liệt kê 3 giao thức khác nhau xuất hiện trong cột giao thức ở bước 7 khi không áp dụng bộ lọc.
2. Mất bao lâu từ khi thông điệp HTTP GET được gửi cho đến khi HTTP OK được nhận (mặc định, giá trị của cột thời gian trong packet-listing window là khoảng thời gian tính bằng giây kể từ khi chương trình Wireshark bắt đầu).
3. Địa chỉ IP của gaia.cs.umass.edu là gì? Địa chỉ IP của máy tính bạn là gì?
4. In 2 thông điệp HTTP (GET và OK) trong câu 2 ở trên (chọn Print từ File menu, chọn Selected Packet Only và Print as displayed, sau đó chọn OK).