



Lab

1

Làm quen với Wireshark

Wireshark Getting Started

Môn học: Nhập môn Mạng máy tính

Tái bản lần 4 - Tháng 09/2021

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Làm quen với phần mềm **Wireshark** – công cụ bắt gói tin phổ biến, phục vụ việc nghiên cứu về hoạt động của các tầng mạng.

2. Kiến thức nền tảng

- Kiến thức về Mạng máy tính cơ bản, nguyên tắc hoạt động của mạng máy tính.

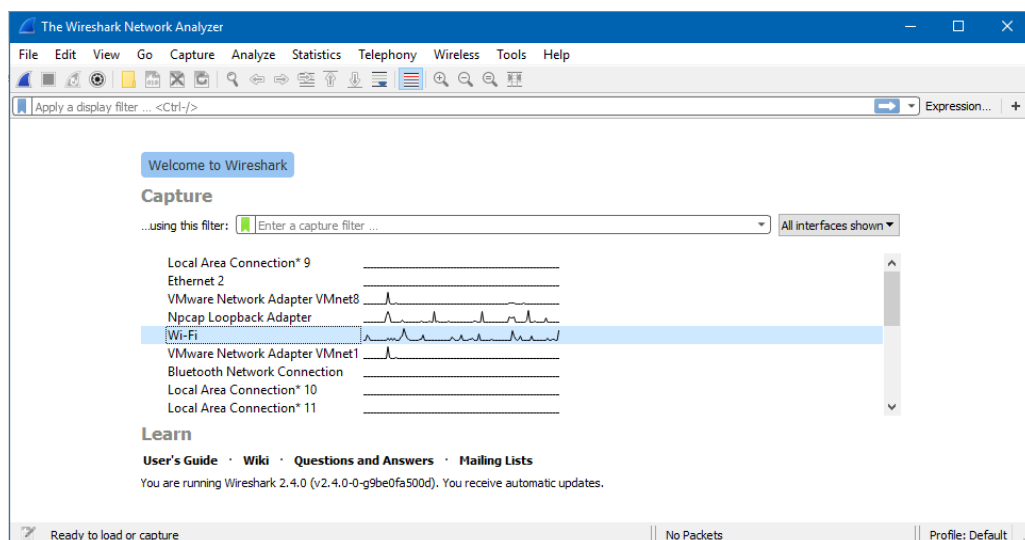
3. Môi trường thực hành

Sinh viên cần chuẩn bị trước máy tính có kết nối Internet và cài đặt các phần mềm:

Phần mềm Wireshark

Đây là phần mềm bắt gói tin trong mạng (sniffing) giúp theo dõi quá trình trao đổi dữ liệu trong mạng. Đối với môn học này, Wireshark giúp phân tích và hiểu rõ hơn hoạt động của các tầng (layer) của mạng.

Tải về bản mới nhất tại <https://www.wireshark.org/download.html>



Hình 1. Giao diện chính của Wireshark

B. THỰC HÀNH

1. Task 1: Mở đầu về Mạng máy tính

➡ Trước khi bắt đầu thực hành, sinh viên hãy trả lời các câu hỏi sau:

- Kể tên các loại thiết bị liên quan đến Mạng mà bạn biết hoặc đang sử dụng tại nơi ở (kèm ảnh minh họa).
- Những vấn đề gì có thể xảy ra nếu không có kết nối Internet trong 5 phút?
- Mục tiêu về kiến thức sau khi hoàn thành môn học Nhập môn Mạng máy tính của bạn là gì?

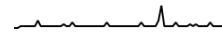
2. Task 2: Làm quen với Wireshark và thử nghiệm bắt gói tin trong mạng

2.1 Giới thiệu và làm quen với Wireshark

Wireshark là phần mềm bắt gói tin (packet sniffer) rất phổ biến và miễn phí chạy trên Windows, Linux, MacOS, hỗ trợ bắt gói tin và quan sát nội dung của các thông điệp được trao đổi bởi các giao thức tại các tầng mạng khác nhau.

Ngoài ra, Wireshark còn phục vụ cho việc điều tra các chứng cứ số (forensic) liên quan đến các vụ án về mạng máy tính.

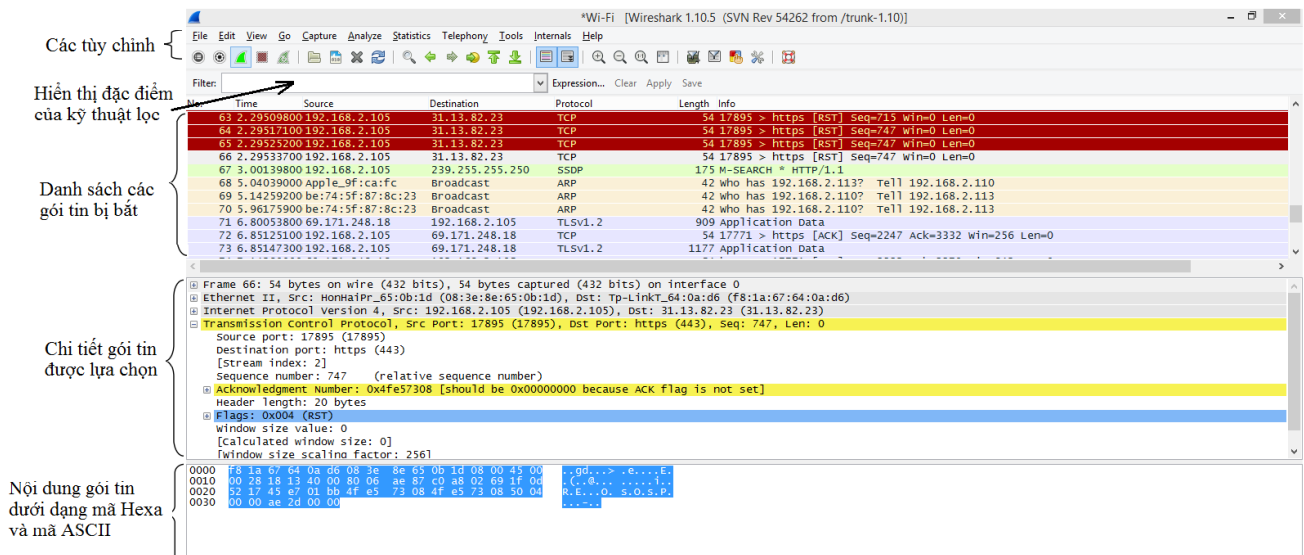
Giao diện chính khi mở Wireshark sẽ giống *Hình 1*.

Tại cửa sổ đầu tiên, bạn sẽ thấy danh sách các card mạng (hay *network interface*) trong mục **Capture**. Quan sát bên phải tên interface sẽ có minh họa thể hiện cho hoạt động trao đổi dữ liệu trong mạng, khi có dấu hiệu như  thì có thể nhận định đang có dữ liệu trao đổi qua interface đó.

Tùy theo loại kết nối và hệ điều hành đang sử dụng, tên của các interface sẽ khác nhau. Ví dụ, tên các interface thông thường trên Windows như sau:

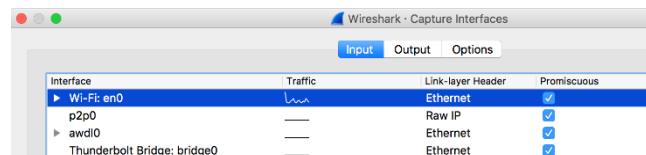
- Kết nối có dây: *Ethernet, Local Area Connection (LAN)*.
- Kết nối không dây: *WiFi*.

Sau đó, giao diện bắt gói tin sẽ xuất hiện như sau.



Hình 2. Giao diện chính của Wireshark trong suốt quá trình bắt và phân tích gói tin

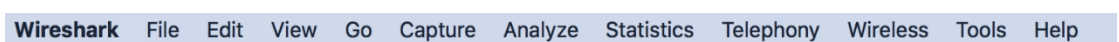
Lưu ý: Để có thể bắt được các gói tin đi qua nó, card mạng cần được kích hoạt chế độ Promiscuous (mặc định sẽ được kích hoạt sẵn trong Wireshark)



Hình 3. Có thể vào Capture > Options để theo dõi cài đặt trên từng interface

Giao diện Wireshark gồm có 5 thành phần chính từ trên xuống:

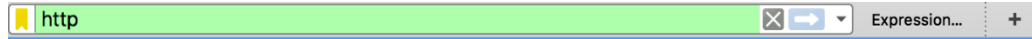
- 1. Command menus:** chứa các menu thực hiện các chức năng chính của Wireshark. Chúng ta quan tâm chủ yếu đến File và Capture.



- **File** menu chứa các tùy chọn cho phép lưu các gói tin đã bắt được (Save) dưới dạng file .pcapng hoặc mở file chứa các gói tin đã bắt từ trước.
- **Capture** menu cho phép bắt đầu bắt gói tin và thay đổi các tùy chỉnh
- **Các button thường dùng:**
 - - Bắt đầu bắt gói tin trên card mạng đã chọn.
 - - Dừng quá trình bắt gói tin
 - - Khởi động lại quá trình bắt gói tin hiện tại
 - - Mở Capture Options để thay đổi các tùy chỉnh
- **Statistics** menu cung cấp những thông tin thống kê có giá trị liên quan đến file capture

2. **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, để lọc các gói tin HTTP (các gói tin liên quan đến việc truy cập web), ta gõ “http” vào khung này và chọn Apply.



3. **Packet-listing windows:**

Hiển thị thông tin tóm tắt cho các gói tin đã bắt, bao gồm:

- No: Số thứ tự (số này được gán bởi Wireshark, không phải số thứ tự chứa trong header của gói tin)
- Time: mốc thời gian gói tin bị bắt.
- Source: địa chỉ nguồn
- Destination: địa chỉ đích.
- Protocol: loại giao thức, chỉ hiển thị giao thức hoạt động ở tầng cao nhất.
- Length: độ dài (kích thước) gói tin.
- Info thông tin đặc tả cho giao thức đó.

4. **Packet details window:**

Cung cấp các thông tin chi tiết về gói tin được chọn từ packet-listing window.

```

▶ Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: Apple_c4:ae:ed (ac:bc:32:c4:ae:ed), Dst: JuniperN_8c:35:b0 (44:f4:77:8c:35:b0)
▶ Internet Protocol Version 4, Src: 192.168.5.58, Dst: 64.233.188.95
▼ Transmission Control Protocol, Src Port: 52702, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
  Source Port: 52702
  Destination Port: 443
  [Stream index: 1]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  [Next sequence number: 1 (relative sequence number)]
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x010 (ACK)

```

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 và cuối cùng là thông tin về giao thức ở tầng cao nhất.

5. **Packet Raw data**

Hiển thị toàn bộ nội dung của gói tin dưới dạng ASCII và hexadecimal.

0000	18 66 da 02 c9 f0 ac bc 32 c4 ae ed 08 00 45 00	·f·····2·····E·
0010	00 38 f3 ee 00 00 40 01 fa ec c0 a8 05 3a c0 a8	·8·····@·····:
0020	05 5f 03 03 2f bf 00 00 00 00 45 00 00 38 3f 6d	·_·/·····E·8?m
0030	00 00 80 11 6f 5e c0 a8 05 5f c0 a8 05 3a c5 13	·····o^·····_·····
0040	08 06 00 24 00 00	···\$.·

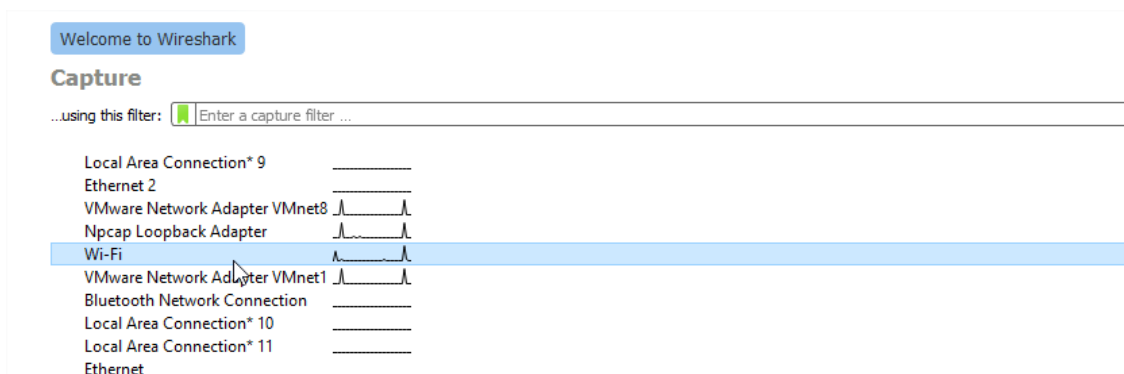
Thực ra, bản chất của mỗi gói tin bắt được chính là phần dữ liệu thô này. Các nội dung hiển thị tại phần 3, 4 do Wireshark phân tích và trực quan hóa để người dùng thuận tiện theo dõi.

2.2 Thử nghiệm bắt gói tin với Wireshark

➔ *Sinh viên thực hành theo các bước sau tại môi trường đã chuẩn bị:*

- **Bước 1:** Khởi động trình duyệt web bất kỳ như *Google Chrome, Firefox, Edge,...* và phần mềm Wireshark (phiên bản mới nhất)
- **Bước 2:** Tại phần **Capture**, chọn interface đang hoạt động chính trên máy để bắt đầu bắt gói tin.

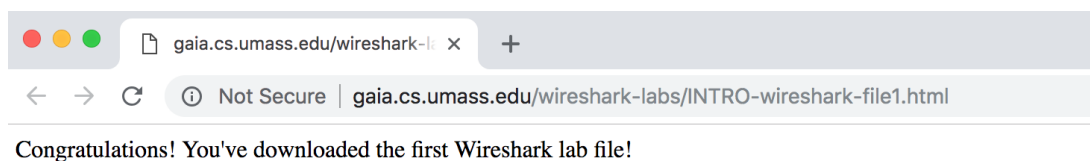
Ví dụ: *Khi đang sử dụng Wifi để kết nối Internet, chọn interface Wifi.*



Hình 4. Chọn interface mạng phù hợp

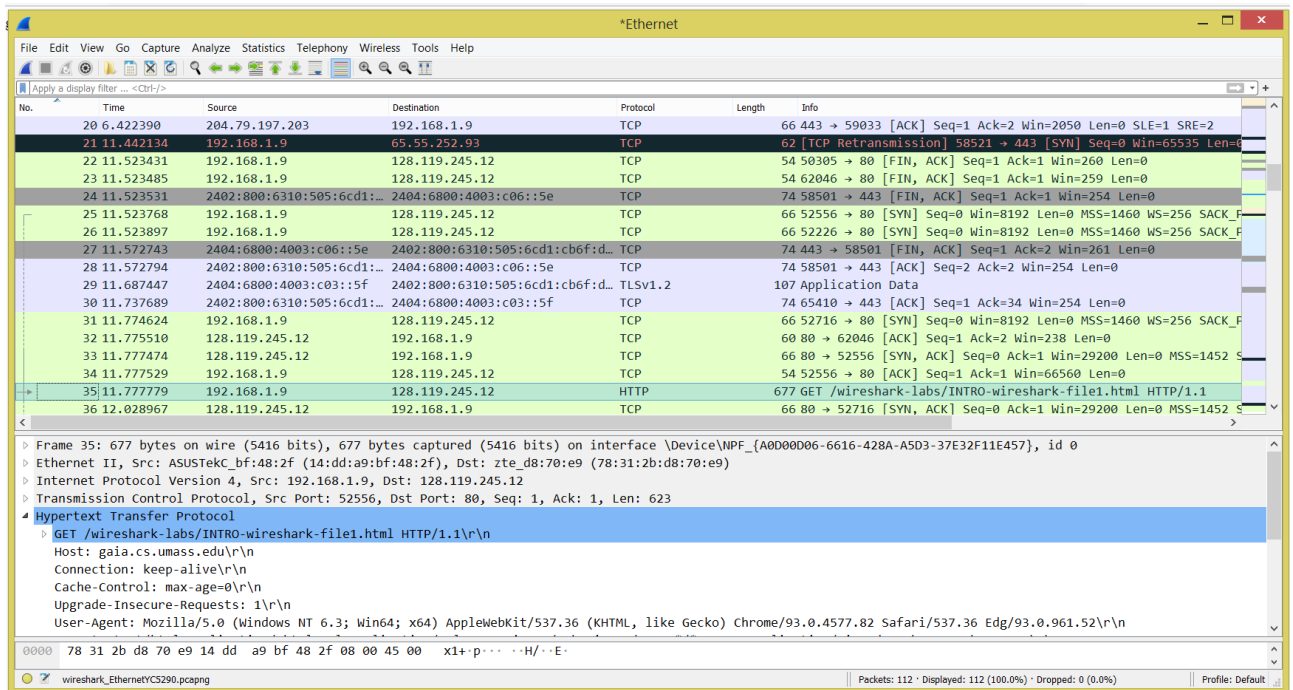
- **Bước 3:** Sau đó, cửa sổ như Hình 4 sẽ xuất hiện và hiển thị kết quả bắt gói tin tại interface đã chọn.
- **Bước 4:** Sử dụng trình duyệt và **chỉ truy cập** vào website có địa chỉ như sau <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

Đây là một website đơn giản có nội dung như sau:



Hình 5. Truy cập website wireshark-file1 thành công

- **Bước 5:** Sau khi trình duyệt đã hiển thị trang INTRO-wireshark-file1.html (chỉ là một dòng chào mừng đơn giản), dừng bắt gói tin tại Wireshark.



Hình 6. Kết quả bắt gói tin sau khi dừng bắt gói tin

Lưu ý: Phải dừng bắt gói tin ngay sau khi đã truy cập thành công vào trang web trên để tránh bắt các gói tin không cần thiết, làm tăng dung lượng file .pcapng khi lưu lại.

Cửa sổ chính của Wireshark bây giờ giống như **Hình 6**. 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 web server **gaia.cs.umass.edu** 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 truy cập một trang web nhưng cũng có nhiều giao thức khác chạy bên dưới mà bạn không thấy được.

- Bước 6: Lưu lại tập tin Wireshark đã bắt được thành file .pcapng có tên dạng *MSSV-Bai1.pcapng*. Ví dụ: *18521006-Bai1.pcapng*.
- Bước 7: Chọn **Start capturing packets** để bắt đầu quá trình bắt gói tin mới.
- Bước 8: Chọn 1 website bất kỳ và lặp lại các bước **4,5,6** với website đó

Lưu ý: Nên chọn website dùng http, không nên chọn website https

Ví dụ: celuit.edu.vn

- Bước 9: Lưu lại tập tin sau khi bắt được ở website thứ 2 thành file pcapng có tên dạng *MSSV-Bai2.pcapng*

2.3 Phân tích kết quả bắt gói tin từ Wireshark

➔ Sinh viên tự thực hiện các bước thực hành như hướng dẫn tại phần 2.2 để có được 2 file kết quả pcapng từ Wireshark. Lần lượt mở từng file tương ứng với 2 website trên và trả lời các câu hỏi sau:

Lưu ý: Trình bày câu trả lời kèm theo ảnh chụp màn hình tương ứng vị trí đã quan sát được thông tin trên Wireshark.

File MSSV-Bai1.pcapng (Lần capture đầu tiên)

1. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?
2. Liệt kê ít nhất **3 giao thức khác nhau** xuất hiện trong cột giao thức (Protocol).
Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.
Gõ “**http**” vào packet-display filter sau đó chọn Apply để Wireshark chỉ hiển thị các thông điệp HTTP trong packet-listing window. Sau đó trả lời các câu hỏi sau:
3. Có bao nhiêu gói tin HTTP? Tỉ lệ % số gói tin HTTP/Tổng số gói tin?
4. Có bao nhiêu gói tin HTTP GET?
(Gợi ý: Quan sát cột Thông tin - Info)
5. Tìm và xác định gói tin HTTP GET đầu tiên được gửi đến web server **gaia.cs.umass.edu**?
(Gợi ý: Quan sát cửa sổ Packet Details – Chi tiết gói tin và trường host)
6. Xác định gói tin phản hồi cho gói HTTP GET ở trên (Câu 5)?
(Gợi ý: Xác định gói tin phản hồi thông qua giá trị **Response in Frame**)
7. Mất bao lâu từ lúc gửi gói tin HTTP GET (Câu 5) đến khi nhận được gói tin phản hồi (Câu 6)?
(Gợi ý: Quan sát Cửa sổ chi tiết gói tin)
8. Dự đoán địa chỉ IP của **gaia.cs.umass.edu** là gì? Địa chỉ IP của máy tính đang sử dụng là gì? Tại sao?
(Gợi ý: Xác định tính chất của việc truy cập Web, bên nào yêu cầu, bên nào phản hồi)

File MSSV-Bai2.pcapng (Lần capture thứ 2)

9. Tổng thời gian bắt gói tin và tổng số gói tin bắt được là bao nhiêu?
10. Liệt kê ít nhất **3 giao thức khác nhau** xuất hiện trong cột giao thức (Protocol).
Tìm hiểu trên Internet và mô tả ngắn gọn chức năng chính của các giao thức đó.
11. Tìm cách để xác định địa chỉ IP của trang web đã chọn ở Bước 8. Địa chỉ IP trang web đã chọn là gì ?
12. Số lượng gói tin và khối lượng dữ liệu được gửi (trao đổi) giữa Địa chỉ trang web ở trên (Câu 11) và máy tính đang sử dụng ?

Gợi ý:

- **Cách 1** – Gõ vào packet-display filter theo mẫu như sau:
`ip.addr==128.63.123.142 && ip.addr==192.168.1.5`
(2 địa chỉ **màu đỏ** và **màu xanh** là địa chỉ IP của trang web và máy tính sử dụng)
- **Cách 2** – *Statistics > Conversations > IPv4 > Tìm dòng thông tin trao đổi giữa 2 địa chỉ IP*

C. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Thực hiện báo cáo cá nhân.
- Sinh viên báo cáo kết quả thực hiện và nộp bài gồm:
 - Báo cáo chi tiết (*lưu ý xuất thành file .PDF*), trình bày cụ thể các yêu cầu trong bài thực hành (có ảnh minh họa) và giải thích các vấn đề kèm theo.
 - 2 file *MSSV-Bai1.pcapng* và *MSSV-Bai2.pcapng* thu được từ việc bắt gói tin bằng Wireshark theo yêu cầu của bài thực hành
 - Nếu có nhiều file, tạo thư mục cùng tên với cùng tên file báo cáo, và đưa tất cả các file ở trên vào Thư mục

Đặt tên file báo cáo theo định dạng như mẫu:

MSSV_HoTen_LabX

Ví dụ: 18521007_NguyenVanA_Lab1

- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

Sinh viên hiểu và tự thực hiện được bài thực hành, trả lời đầy đủ các yêu cầu đặt ra, khuyến khích trình bày báo cáo chi tiết, rõ ràng.

D. TÀI LIỆU THAM KHẢO

Bài thực hành được xây dựng dựa trên *Wireshark Lab: Getting Started* - Supplement to Computer Networking: A Top-Down Approach, 7th ed., J.F Kurose and K.W Ross.

HẾT

Chúc các em hoàn thành tốt