**TRƯỜNG ĐẠI HỌC KINH TẾ**

**ĐẠI HỌC ĐÀ NẴNG**

–––––––––––––––––––––––––––––––



**BÁO CÁO BÀI TẬP**

**CHỦ ĐỀ: KỸ THUẬT BẮT VÀ PHÂN TÍCH GÓI TIN BẰNG WIRESHARK**

**HỌC PHẦN: AN TOÀN VÀ BẢO MẬT HỆ THỐNG THÔNG TIN**

***Tên nhóm*** :  9

***Sinh viên thực hiện*** : Trương Thu Sương (100%)

Nguyễn Thị Mỹ Cương (100%)

Nguyễn Dương Trung (100%)

Trần Khánh Tùng (100%)

Hồ Đăng Đạt (100%)

Nguyễn Thị Tường Vi (100%)

***Giảng viên hướng dẫn*** : Th.s Trần Thị Thu Thảo

**Đà Nẵng, 10/2023**

**Bảng đánh giá phần trăm đóng góp thành viên nhóm**

|  |  |  |
| --- | --- | --- |
| Họ và Tên | Công việc | Phần trăm đóng góp |
| Nguyễn Dương Trung | Làm word + nội dung | 100% |
| Trần Khánh Tùng | Làm demo + nội dung | 100% |
| Trương Thu Sương | Làm slide + nội dung | 100% |
| Nguyễn Thị Mỹ Cương | Làm demo + nội dung | 100% |
| Hồ Đăng Đạt | Làm slide + nội dung | 100% |
| Nguyễn Thị Tường Vi | Làm demo + nội dung | 100% |

**MỤC LỤC**

[Lời Mở Đầu 5](#_Toc149679453)

[I) Giới thiệu phần mềm Wireshark 6](#_Toc149679454)

[1) Giới thiệu 6](#_Toc149679455)

[2) Tính năng của Wireshark 6](#_Toc149679456)

[3) Mục đích sử dụng Wireshark 6](#_Toc149679457)

[II) Hướng dẫn cài đặt và các thành phần cơ bản trong Wireshark 7](#_Toc149679458)

[1) Hướng dẫn cài đặt 7](#_Toc149679459)

[a) Yêu cầu hệ thống 7](#_Toc149679460)

[b) Cách cài đặt 8](#_Toc149679461)

[2) Các thành phần cơ bản trong Wireshark 10](#_Toc149679462)

[a) Cửa sổ chính 10](#_Toc149679463)

[b) Menu 11](#_Toc149679464)

[c) Thanh công cụ chính 12](#_Toc149679465)

[d) Thanh công cụ “bộ lọc” 12](#_Toc149679466)

[e) Ngăn “Packet list” 13](#_Toc149679467)

[f) Ngăn “Packet Details” 13](#_Toc149679468)

[g) Ngăn “Packet Bytes” 13](#_Toc149679469)

[h) Thanh trạng thái 14](#_Toc149679470)

[III) Các giao thức phổ biến được hỗ trợ bởi Wireshark 14](#_Toc149679471)

[1) Giao thức HTTP 14](#_Toc149679472)

[2) Giao thức TCP 15](#_Toc149679473)

[3) Giao thức IP 16](#_Toc149679474)

[4) Giao thức ICMP 16](#_Toc149679475)

[5) Giao thức UDP 16](#_Toc149679476)

[6) Giao thức DNS 17](#_Toc149679477)

[7) Giao thức ARP 17](#_Toc149679478)

[IV) Phân tích gói tin 18](#_Toc149679479)

[1) Thành phần của gói tin 18](#_Toc149679480)

[2) Phân tích gói tin tốt, xấu 19](#_Toc149679481)

[V) Hướng dẫn sử dụng 20](#_Toc149679482)

[1) Cách bắt các gói tin trực tiếp trong Wireshark 20](#_Toc149679483)

[2) Cách lưu và mở gói tin trong Wireshark 23](#_Toc149679484)

[3) Cách xem các gói tin trong Wireshark 24](#_Toc149679485)

[4) Cách lọc các gói tin trong Wireshark 24](#_Toc149679486)

[5) Cách Color Coding trong Wireshark 27](#_Toc149679487)

[VI) Một số tính năng nâng cao của Wireshark 28](#_Toc149679488)

[1) Following TCP Streams 28](#_Toc149679489)

[2) Cửa sổ thống kê phân cấp giao thức 29](#_Toc149679490)

[3) Đồ thị IO 30](#_Toc149679491)

[VII) Ưu điểm, nhược điểm của Wireshark 31](#_Toc149679492)

[1) Ưu điểm của Wireshark 31](#_Toc149679493)

[2) Nhược điểm của Wireshark 31](#_Toc149679494)

[VIII) Đánh giá, kết luận 32](#_Toc149679495)

[1) Đánh giá 32](#_Toc149679496)

[2) Kết luận 32](#_Toc149679497)

# **Lời Mở Đầu**

Ở thời đại công nghệ thông tin đang phát triển cực mạnh như hiện nay đã mở ra sự giao tiếp cực lớn giữa mạng máy tính và con người. Song song đó nó vẫn mang theo những rủi ro đáng lưu tâm. Đối mặt với những thách thức ngày càng phức tạp của môi trường mạng, quá trình hiểu rõ và giám sát các gói tin mạng trở nên quan trọng hơn bao giờ hết.

Mỗi ngày, dữ liệu được truyền đi qua những con hẻm chật hẹp, khác với sự hào nhoáng mà thành phố ảo này đã phô diễn ra cho ta thấy. Tương tự vậy, liệu trong số chúng ta đã có ai từng đặt ra câu hỏi rằng dưới bề mặt mạng kia sẽ thực sự chứa đựng những điều bí ẩn nào mà con người vẫn chưa nhìn thấy được? Và từ đó, Wireshark ra đời. Nó là công cụ dùng để phân tích gói tin mạnh mẽ nhất, cho phép chúng ta bắt, xem xét và hiểu rõ từng ngôn ngữ mà mạng sử dụng để giao tiếp.Và để hiểu rõ hơn và có thể sử dụng Wireshark một cách thuần thục nhất, thì chúng ta hãy cùng phân tích và nghiên cứu Wireshark thông qua bài báo cáo của nhóm chúng mình. Trong quá trình nghiên cứu và trình bày có điều gì sai sót mong thầy cô giúp đỡ để bài nghiên cứu được hoàn thành một cách tốt nhất. Xin cảm ơn các thầy cô.

1. **Giới thiệu phần mềm Wireshark**
2. **Giới thiệu**

* Wireshark là một công cụ phân tích gói tin mã nguồn mở và miễn phí. Công cụ này được sử dụng để bắt, phân tích và ghi lại lưu lượng mạng. Wireshark có thể được sử dụng để xác định các vấn đề về mạng, chẳng hạn như kết nối chậm, rớt gói tin hoặc các truy cập bất thường. Công cụ này cũng có thể được sử dụng để phát triển và thử nghiệm các ứng dụng mạng. Wireshark hoạt động bằng cách bắt tất cả lưu lượng mạng đi qua giao diện mạng được chọn. Công cụ này sau đó phân tích lưu lượng mạng và hiển thị thông tin về các gói tin

1. **Tính năng của Wireshark**

* Phân tích được rất nhiều giao thức : UTP, UDP, HTTP…
* Sử dụng được trên nhiều hệ điều hành : Win, MacOS, Linux…
* Chụp trực tiếp dữ liệu của gói tin ngay trên dữ liệu và có thể phân tích offline
* Hiển thị các gói tin với thông tin của giao thức rất chi tiết
* Lưu dữ liệu của các gói tin đã bắt được
* Lọc và tìm kiếm gói tin với nhiều điều kiện
* Bắt (capture) tất cả dữ liệu của Ethernet, Bluetooth, USB, Frame Relay, FDDI, IEEE 802.11, PPP/HDLC, ATM, Token Ring, …
* Phân giải tên : Đây là quá trình chuyển đổi địa chỉ dài và khó ghi nhớ thành một địa chỉ khác đơn giản hơn
* Following TCP streams : tính năng này vô cùng hữu ích, nó cho phép bạn phối hợp các thông tin liên quan đến các gói tin và cho bạn dữ liệu cuối cùng cả người dùng nhìn thấy trong ứng dụng

1. **Mục đích sử dụng Wireshark**

* Phân tích và gỡ lỗi mạng: Phần mềm này cho phép người dùng xem và phân tích các gói tin mạng để xác định nguyên nhân gây ra sự cố mạng, như kết nối chậm, lỗi giao thức, mất dữ liệu và các vấn đề khác. Điều này giúp kỹ thuật viên mạng tìm ra và giải quyết các vấn đề mạng một cách hiệu quả.
* Kiểm tra bảo mật mạng: Wireshark có khả năng phân tích và hiển thị dữ liệu trong các gói tin mạng, cho phép người dùng kiểm tra bảo mật mạng bằng cách phát hiện và theo dõi các hoạt động không mong muốn, tấn công mạng, hoặc các thông tin nhạy cảm đang được truyền qua mạng.
* Phân tích hiệu suất mạng: Phần mềm này cung cấp các công cụ phân tích mạnh mẽ để đo lường và đánh giá hiệu suất mạng, bao gồm độ trễ, tốc độ truyền dữ liệu, thời gian đáp ứng và các tham số khác. Điều này giúp người dùng xác định và cải thiện hiệu suất mạng để đảm bảo hoạt động mạng tối ưu.
* Giảng dạy và nghiên cứu: Wireshark là công cụ quan trọng trong việc giảng dạy và nghiên cứu về mạng máy tính. Nó cho phép người dùng tìm hiểu về các giao thức mạng, quá trình truyền thông, cấu trúc gói tin và các khía cạnh kỹ thuật khác liên quan đến mạng.

1. **Hướng dẫn cài đặt và các thành phần cơ bản trong Wireshark**
2. **Hướng dẫn cài đặt**
3. **Yêu cầu hệ thống**

* Wireshark sẽ hoạt động với mọi phiên bản Windows vẫn đang trong thời gian hỗ trợ mở rộng. Wireshark hiện hỗ trợ Windows 11, 10, 8.1, 8, Server 2019, Server 2016, Server 2012 R2 và Server 2012. Cũng cần có các yêu cầu sau:

+ Kiến trúc CPU AMD64/x86-64 64-bit hoặc 32-bit x86.

+ Ít nhất 500 MB RAM có sẵn. Nó đòi hỏi nhiều RAM hơn để xử lý các tệp chụp lớn hơn.

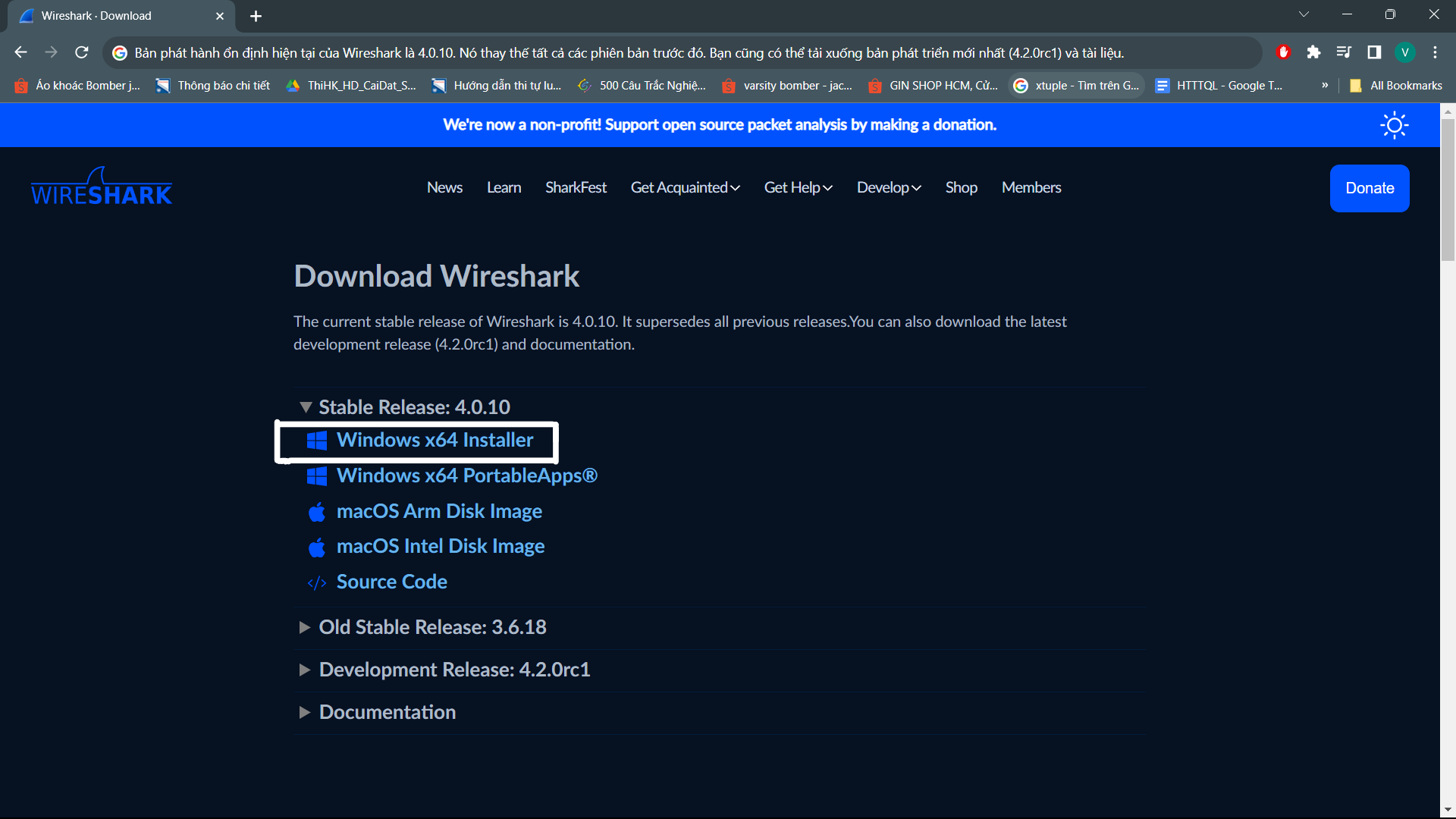
+ Ít nhất 500 MB dung lượng đĩa trống. Các tập tin chụp yêu cầu thêm dung lượng đĩa.

+ Nó yêu cầu độ phân giải tối thiểu là 1280 × 1024 hoặc cao hơn.

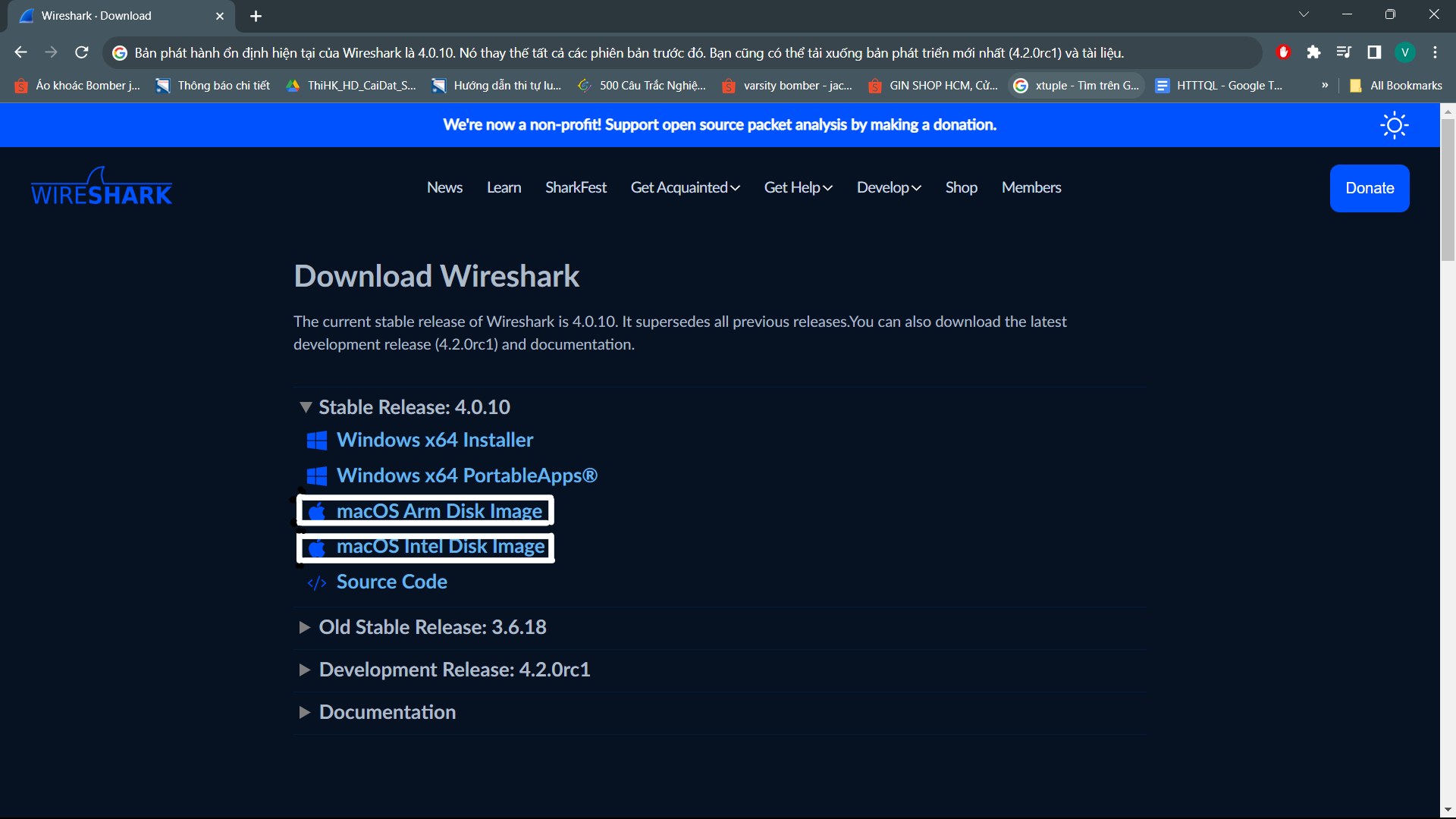
1. **Cách cài đặt**

* Đối với Windows:

Có thể tải trực tiếp tại trang chủ của Wireshark, phần mềm này có hỗ trợ Windows phiên bản 32 bit và 64 bit. Hãy chọn phiên bản chính xác cho hệ điều hành đang sử dụng. Bản phát hành ổn định hiện tại của Wireshark là 4.0.10. Nó thay thế tất cả các phiên bản trước đó. Bạn cũng có thể tải xuống bản phát triển mới nhất (4.2.0rc1) và tài liệu. Sau khi tài về thì giải nén và sử dụng



* Đối với MacOS: Bản cài đặt chính thức cho macOS đã được hỗ trợ trên trang chủ chính thức của Wireshark, chỉ việc download và mở file .dmg để bắt đầu cài đặt, kéo thả biểu tượng của Wireshark vào thư mục/Applications để hoàn tất.



* Đối với Kali Linux:

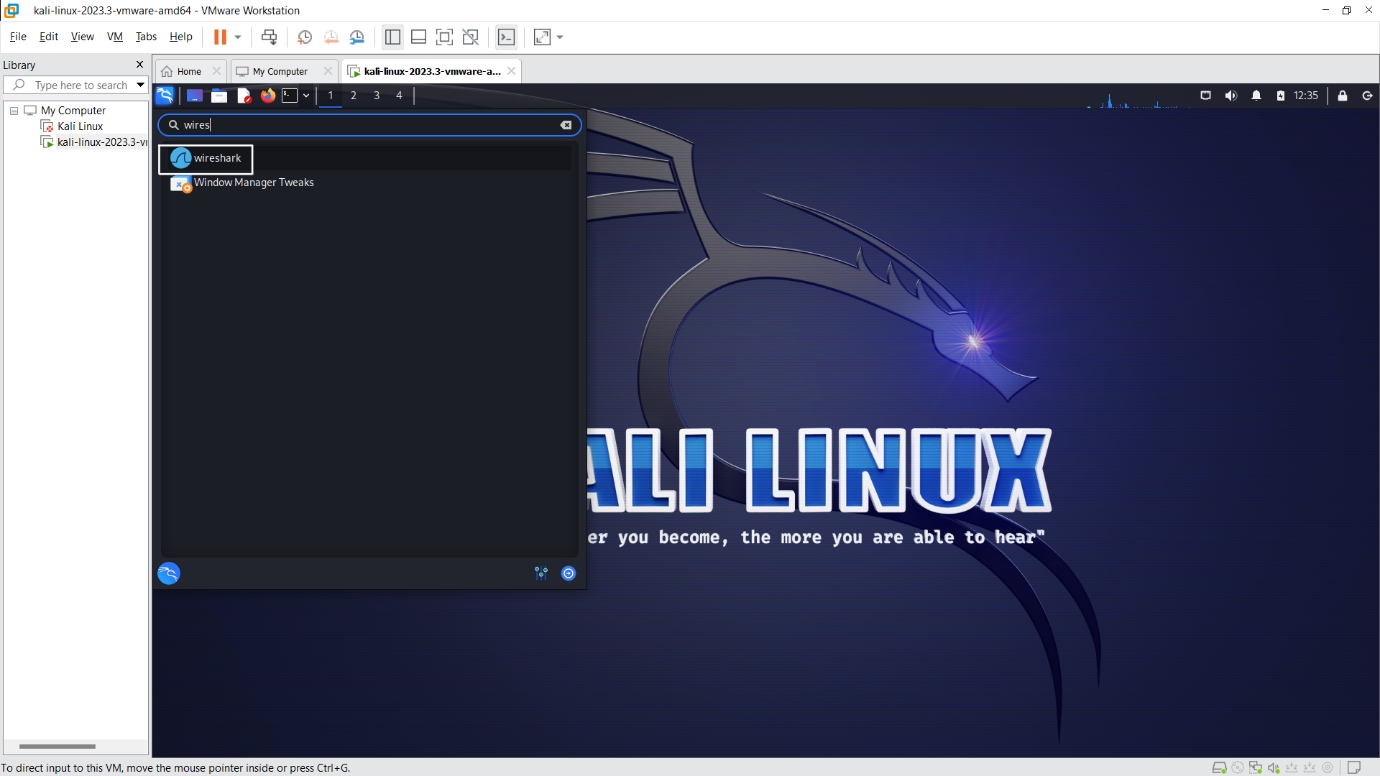
B1: Để sử dụng được Wireshark trong Kali Linux. Đầu tiên ta phải tải phần mềm máy ảo VMware tại trang chủ chính thức của VMware và tải tập tin chứa hệ điều hành Kali Linux tại trang chủ của Kali Linux

B2: Giải nén và cài đặt file VMware

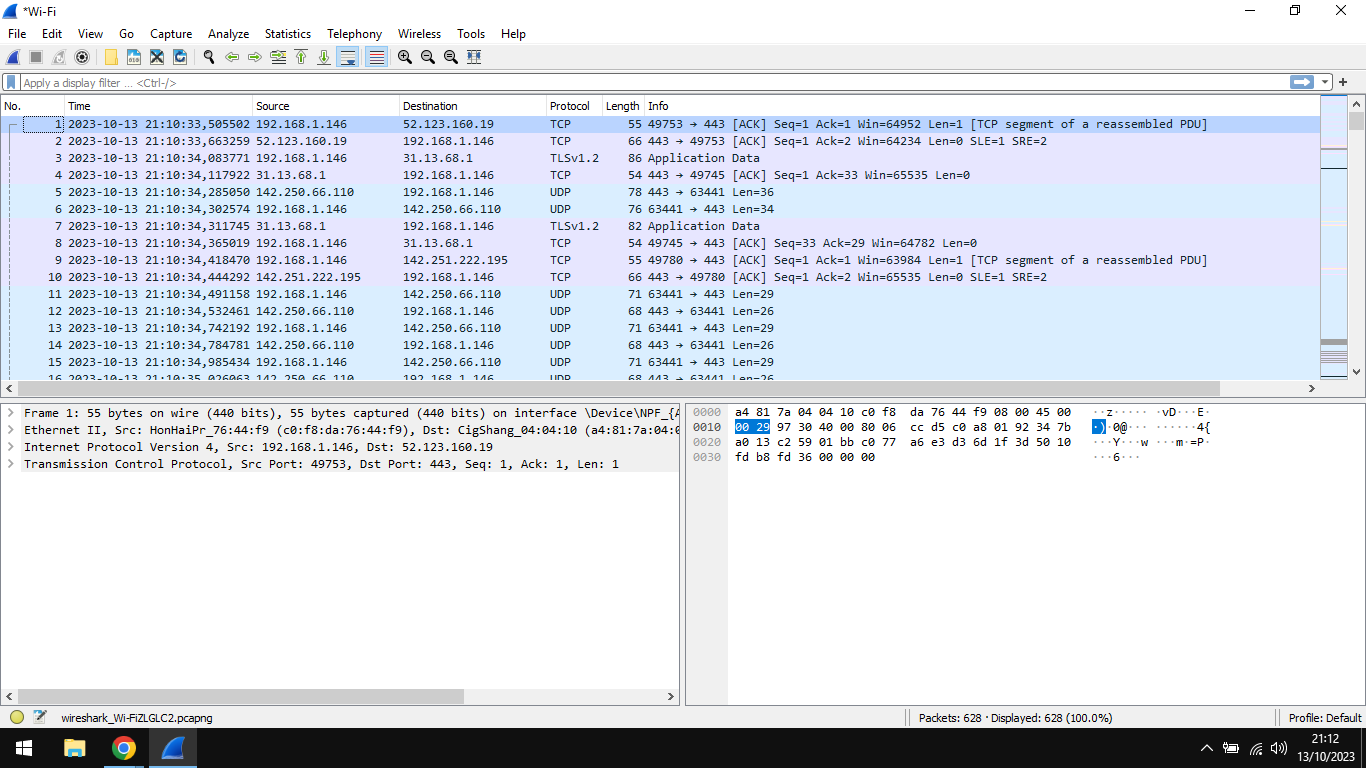
B3: Khởi tạo máy ảo Kali Linux

B4: Khởi động máy ảo Kali Linux, mở Applications và chọn tìm Wireshark ở thanh tìm kiếm

B5: Mở Wireshark và sử dụng



1. **Các thành phần cơ bản trong Wireshark**
2. **Cửa sổ chính**

* Giao diện cửa sổ chính của Wireshark sẽ được hiển thị như hình dưới đây

1. **Menu**

* Thanh menu chính sẽ chứa các mục như sau:



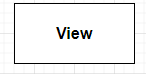
* Menu File: Menu này sẽ chứa các mục Open, Save, Print, Export, Quit,...



* Menu Edit: Menu này chứa các mục find a packet, time reference hoặc đánh dấu một hoặc nhiều gói tin, xử lý các cấu hình và đặt tùy chọn của người dùng.



* Menu View: Menu này cho phép người dùng xem được những gì sẽ hiển thị ra màn hình chính



* Menu Go: Menu này chứa các mục để chuyển đến một gói cụ thể như Back, Forward , Go to Packet



* Menu Capture: Menu này cho phép bạn bắt đầu và dừng bắt gói tin và chỉnh sửa các bộ lọc.



* Menu Analyze: Menu này chứa các mục để thao tác các bộ lọc, bật hoặc tắt phân tích các giao thức, giải mã và theo dõi luồng.



* Menu Statistics: Menu này sẽ hiển thị các cửa sổ thống kê khác nhau bao gồm tóm tắt các gói đã được thu thập, hiển thị thống kê phân cấp giao thức và nhiều công dụng khác.



* Menu Telephony: Menu này chứa các mục để hiển thị các thống kê mạng liên quan đến điện thoại.



* Menu Wireless: Menu này chứa các mục để hiển thị thống kê không dây Bluetooth.



* Menu Tools: Menu này chứa các công cụ khác nhau có sẵn trong Wireshark, chẳng hạn như tạo Quy tắc ACL tường lửa.



* Menu Help: Menu này chứa các mục để giúp người dùng, chẳng hạn như truy cập vào một số trợ giúp cơ bản, các trang hướng dẫn sử dụng các công cụ dòng lệnh khác nhau, truy cập trực tuyến vào một số trang web và hộp thoại giới thiệu thông thường.



1. **Thanh công cụ chính**

* Thanh công cụ chính cho phép truy cập nhanh vào các mục thường dùng từ menu.

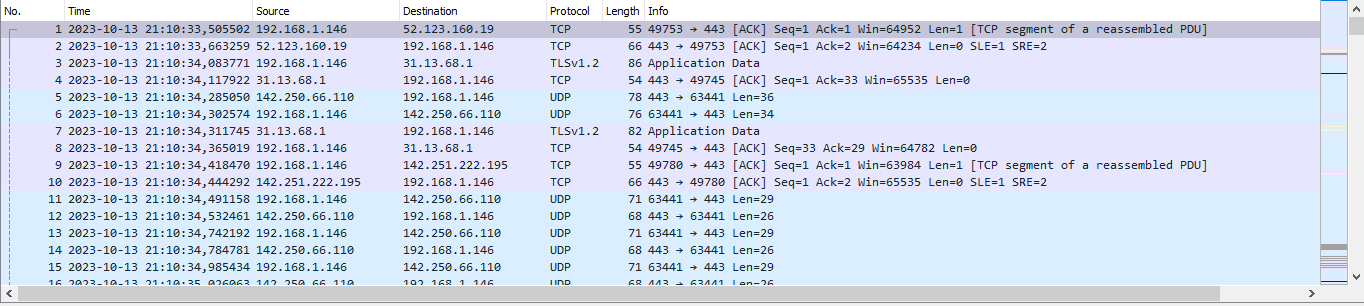


1. **Thanh công cụ “bộ lọc”**

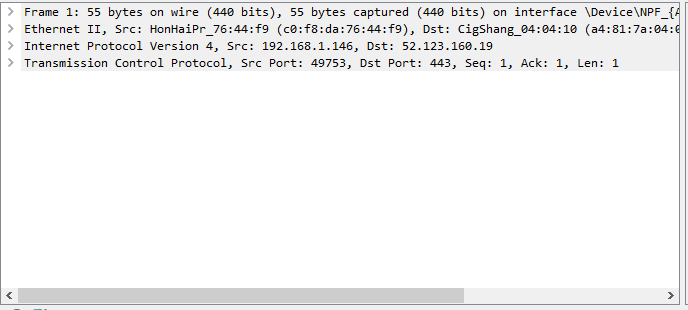
* Thanh công cụ bộ lọc cho phép người dùng đặt bộ lọc hiển thị để lọc gói nào được hiển thị.



1. **Ngăn “Packet list”**

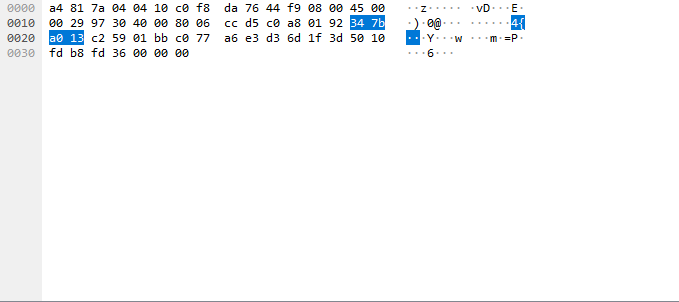
* Ngăn danh sách gói hiển thị một bản tóm tắt của mỗi gói tin được thu thập. Bằng cách nhấp vào các gói trong ngăn này, người dùng kiểm soát những gì được hiển thị trong hai ngăn còn lại.

1. **Ngăn “Packet Details”**

* Ngăn chi tiết hiển thị chi tiết hơn về gói được chọn trong ngăn danh sách gói. Ngăn này hiển thị các giao thức và trường giao thức của gói được chọn.

1. **Ngăn “Packet Bytes”**

* Ngăn byte hiển thị dữ liệu từ gói tin được chọn trong Packet List và đánh dấu trường được chọn trong Packet Details và hiển thị dưới dạng hexdump.



1. **Thanh trạng thái**

* Thanh trạng thái hiển thị một số thông tin chi tiết về trạng thái chương trình hiện tại và dữ liệu đã thu thập.

1. **Các giao thức phổ biến được hỗ trợ bởi Wireshark**

Wireshark là một công cụ phân tích gói dữ liệu mạng mạnh mẽ, có khả năng hỗ trợ và phân tích nhiều giao thức mạng khác nhau. Và cũng bởi Wireshark được phát triển trên mô hình mã nguồn mở, những giao thức mới sẽ được thêm vào.Dưới đây là một số ví dụ về các giao thức thường được sử dụng trong WireShark

1. **Giao thức HTTP**

HTTP (Hypertext Transfer Protocol) là một giao thức truyền tải dữ liệu trên mạng, thường được sử dụng cho việc truyền tải trang web, dữ liệu và tài liệu liên quan qua mạng Internet. HTTP hỗ trợ nhiều phương thức, trong đó hai phương thức phổ biến nhất là GET và POST. Phương thức GET được sử dụng để lấy dữ liệu từ máy chủ, trong khi POST được sử dụng để gửi dữ liệu lên máy chủ. Ngoài ra thì HTTP cũng là một giao thức ứng dụng của bộ [giao thức TCP/IP](https://blogchiasekienthuc.com/dan-cong-nghe/mo-hinh-osi-va-tcp-ip.html) (đây là các giao thức nền tảng cho Internet). Và thường thì giao thức HTTP sử dụng cổng 80 (Port 80) là chủ yếu. HTTP được sử dụng để truyền tải dữ liệu giữa web server đến các [trình duyệt web](https://blogchiasekienthuc.com/phan-mem-mien-phi/trinh-duyet-web-tot-nhat.html) mà bạn đang sử dụng, chẳng hạn như Microsoft Edge, Google Chrome, Safari, Cốc Cốc hay là FireFox…

HTTP hoạt động bằng cách bắt đầu kết nối TCP đến máy chủ. Các phiên duyệt web sử dụng cổng máy chủ 80 theo mặc định, mặc dù các cổng khác như 8080 đôi khi cũng được sử dụng thay thế. Sau khi phiên được thiết lập, bạn kích hoạt gửi và nhận tin nhắn HTTP bằng cách truy cập trang web.

1. **Giao thức TCP**

Transmission Control Protocol (TCP) là giao thức tiêu chuẩn trên Internet đảm bảo trao đổi thành công các gói dữ liệu giữa các thiết bị qua mạng. TCP là giao thức truyền tải cơ bản cho nhiều loại ứng dụng, bao gồm máy chủ web và trang web, ứng dụng email, FTP và các ứng dụng ngang hàng.

TCP hoạt động với giao thức Internet (IP) để chỉ định cách dữ liệu được trao đổi trực tuyến. IP chịu trách nhiệm gửi từng gói đến đích của nó, trong khi TCP đảm bảo rằng các byte được truyền theo thứ tự mà chúng được gửi mà không có lỗi hoặc thiếu sót nào. Hai giao thức kết hợp với nhau được gọi là TCP/IP.

TCP hoạt động theo tiến trình bắt tay 3 bước (3 way handshake).

* Máy khách gửi cho máy chủ một gói SYN — một yêu cầu kết nối từ port nguồn của nó đến port đích đến của máy chủ.
* Máy chủ phản hồi bằng gói SYN/ACK, xác nhận việc nhận được yêu cầu kết nối.
* Máy khách nhận gói SYN/ACK và trả lời bằng gói ACK của chính nó.

1. **Giao thức IP**

IP (Internet Protocol - giao thức Internet) là là một giao thức mạng lớp mạng của mô hình tham chiếu OSI. IP chịu trách nhiệm định tuyến dữ liệu trong mạng Internet. IP cung cấp một địa chỉ duy nhất cho mỗi máy tính trong mạng. Địa chỉ IP này được sử dụng để định tuyến dữ liệu từ máy tính nguồn đến máy tính đích. Vai trò của IP tương tự vai trò của giao thức tầng mạng trong mô hình IOS. Mặc dù Internet xuất hiện trong IP nhưng giao thức này không nhất thiết phải sử dụng Internet. Tất cả các máy trạm trên Internet đều hiểu IP, nhưng IP có thể sử dụng trong các mạng mà không có sự liên hệ với Internet. IP là giao thức kiểu không kết nối, tức là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

1. **Giao thức ICMP**

ICMP ( Internet Control Message Protocol ), là một giao thức của gói Internet Protocol. Giao thức này được các thiết bị mạng như router dùng để gửi đi các thông báo lỗi chỉ ra một dịch vụ có tồn tại hay không, hoặc một địa chỉ host hay router có tồn tại hay không.

Giao thức tin nhắn được kiểm soát trên Internet (ICMP) thường hoạt động cùng với các giao thức mạng khác như TCP/IP hoặc Giao thức dữ liệu người dùng (UDP). Máy chủ và bộ định tuyến trao đổi tin nhắn ICMP hoặc gói ICMP khi xảy ra một số sự kiện mạng nhất định. Một gói ICMP bao gồm một tiêu đề gói ICMP và một phần dữ liệu ICMP.

1. **Giao thức UDP**

UDP (User Datagram Protocol) là một trong những giao thức cốt lõi của giao thức TCP/IP. Theo dõi giao thức UDP, xác định cổng nguồn và đích, và hiển thị các gói dữ liệu UDP trao đổi giữa các máy tính.

Giao thức UDP hoạt động tương tự như TCP nhưng nó không cung cấp kiểm tra lỗi khi truyền gói tin.

Khi một ứng dụng sử dụng UDP, các gói tin chỉ được gửi đến người nhận. Người gửi không đợi để đảm bảo người nhận nhận được gói tin hay không, mà nó tiếp tục gửi các gói tiếp theo. Nếu người nhận bỏ lỡ một vài gói tin UDP, gói tin đó bị mất vì người gửi sẽ không gửi lại chúng. Điều này có nghĩa là các thiết bị có thể giao tiếp nhanh hơn.

1. **Giao thức DNS**

**DNS (**Domain **Name Server)**là một giao thức tiêu chuẩn cho phép bạn nhập địa chỉ của một trang Web và tự động khám phá địa chỉ giao thức Internet (IP) cho trang Web đó.

Có rất nhiều máy chủ DNS lưu trữ tất cả các bản ghi DNS cho Internet. Bất kỳ máy tính nào muốn biết số hoặc tên đều có thể hỏi máy chủ DNS của họ. Máy chủ DNS của bạn cũng biết cách hỏi, hoặc truy vấn các máy chủ DNS khác khi chúng cần bản ghi. Khi một máy chủ DNS truy vấn các máy chủ DNS khác, nó sẽ thực hiện một truy vấn ngược dòng.

Máy chủ định danh có thẩm quyền là nơi quản trị viên quản lý tên máy chủ và địa chỉ IP cho miền của họ. Bất cứ khi nào quản trị viên DNS muốn thêm, thay đổi hoặc xóa tên máy chủ hoặc địa chỉ IP, họ sẽ thực hiện thay đổi trên máy chủ DNS có thẩm quyền của mình (đôi khi được gọi là Master DNS Server). Ngoài ra, còn có các Slave DNS Server. Các máy chủ DNS này giữ bản sao của các bản ghi DNS cho các vùng và tên miền của chúng.

1. **Giao thức ARP**

ARP (Address Resolution Protocol) đây là một thủ tục để kết nối một địa chỉ IP động tới một server vật lý cố định trong mạng Lan (còn gọi là địa chỉ Mac).

Hiện tại phổ biến nhất là địa chỉ IP4 ([Ipv4](https://bkhost.vn/blog/ipv4/)) với độ dài là 32 bit. Trong khi đó địa chỉ Mac lại 48 bit. Chính vì sự khác biệt đó mà ARP cần phải ánh xạ để phiên dịch 32 bit thành 48 bit và ngược lại. Quá trình mapping của ARP giữ chức năng quan trọng để các hệ thống nhận ra nhau và bảo mật một cách trọn vẹn, an toàn.

Quá trình hoạt động của ARP sẽ bắt đầu khi một gói tin được gửi tới cho một máy chủ nào đó trong [mạng LAN](https://bkhost.vn/blog/mang-lan/). Chương trình ARP cần tìm địa chỉ Mac khớp với địa chỉ IP của gói tin ở bảng ARP [cache](https://bkhost.vn/blog/cache-la-gi/) (bản ghi từng địa chỉ Mac và địa chỉ IP tương ứng).

Nếu địa chỉ Mac có trong ARP cache thì thiết bị nguồn sẽ sử dụng địa chỉ Mac ở đó để giao tiếp. Trường hợp trong ARP cache không có địa chỉ mà nguồn muốn tìm thì ARP sẽ gửi một thông báo tới các máy trong mạng LAN để xem máy nào có địa chỉ IP khớp với địa chỉ IP đích. Khi một máy nhận ra địa chỉ IP đích khớp với IP của chính nó thì nó sẽ trả lời để ARP cập nhật vào bộ nhớ ARP cache và tiếp tục giao tiếp.

1. **Phân tích gói tin**
2. **Thành phần của gói tin**

Gói tin trong Wireshark là một đơn vị dữ liệu được truyền qua mạng. Gói tin bao gồm các thành phần sau:  
- Tiêu đề gói tin: Tiêu đề gói tin chứa thông tin cơ bản về gói tin, chẳng hạn như địa chỉ nguồn, địa chỉ đích, giao thức, v.v.  
- Dữ liệu gói tin: Dữ liệu gói tin chứa thông tin thực tế được truyền qua mạng.  
Tiêu đề gói tin được chia thành các trường khác nhau, mỗi trường chứa một loại thông tin cụ thể. Dưới đây là một số trường tiêu đề gói tin phổ biến:  
- Địa chỉ nguồn: Địa chỉ nguồn là địa chỉ IP của máy tính gửi gói tin.  
- Địa chỉ đích: Địa chỉ đích là địa chỉ IP của máy tính nhận gói tin.  
- Giao thức: Giao thức là loại giao thức được sử dụng để truyền gói tin.  
- Cổng nguồn: Cổng nguồn là cổng TCP hoặc UDP của máy tính gửi gói tin.  
- Cổng đích: Cổng đích là cổng TCP hoặc UDP của máy tính nhận gói tin.  
- Kích thước gói tin: Kích thước gói tin là kích thước của gói tin, tính bằng byte.  
- Dữ liệu gói tin có thể được trình bày ở định dạng nhị phân hoặc văn bản. Trong định dạng nhị phân, dữ liệu gói tin được hiển thị dưới dạng một chuỗi các số thập lục phân. Trong định dạng văn bản, dữ liệu gói tin được hiển thị dưới dạng văn bản.

1. **Phân tích gói tin tốt, xấu**

* Gói tin tốt là gói tin được gửi đi và nhận về một cách chính xác, không bị lỗi hoặc bị tấn công.
* Gói tin xấu là gói tin bị lỗi hoặc bị tấn công, có thể gây ra các vấn đề như rò rỉ dữ liệu, mất dữ liệu, hoặc gián đoạn dịch vụ.

Để phân biệt gói tin tốt xấu trong Wireshark, người dùng có thể sử dụng các tiêu chí sau:

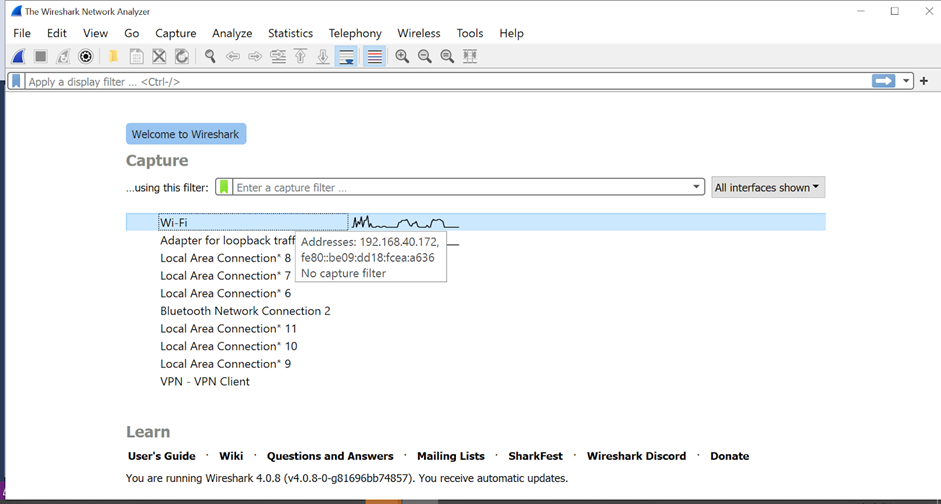
* Trạng thái gói tin: Gói tin tốt sẽ có trạng thái là OK. Gói tin xấu có thể có trạng thái là Error, Unknown, Invalid, hoặc Dropped.
* Tiêu đề gói tin: Gói tin tốt sẽ có các trường tiêu đề được điền đầy đủ và chính xác. Gói tin xấu có thể có các trường tiêu đề bị thiếu, bị lỗi, hoặc bị sửa đổi.
* Nội dung gói tin: Gói tin tốt sẽ có nội dung được truyền đi và nhận về một cách chính xác. Gói tin xấu có thể bị thay đổi hoặc bị xóa bỏ.

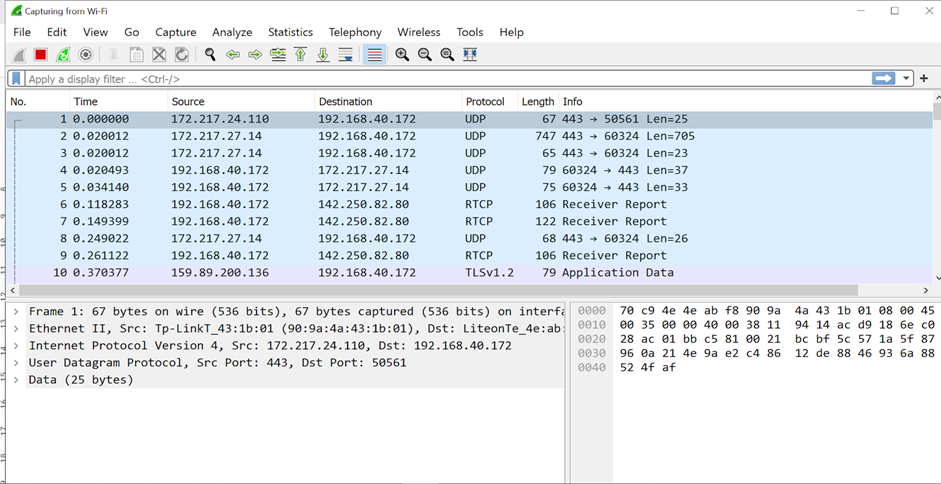
Dưới đây là một số ví dụ về gói tin xấu:

* Gói tin bị lỗi: Gói tin bị lỗi là gói tin có các trường tiêu đề hoặc nội dung bị lỗi. Ví dụ, gói tin có thể bị mất một số byte dữ liệu, hoặc có thể có các byte dữ liệu bị thay đổi.
* Gói tin bị tấn công: Gói tin bị tấn công là gói tin được gửi đi với mục đích gây hại. Ví dụ, gói tin có thể được sử dụng để đánh cắp dữ liệu, hoặc để phá hoại hệ thống.
* Tấn công từ chối dịch vụ (DoS): Gói tin DoS thường được gửi với số lượng lớn đến một máy chủ hoặc dịch vụ, với mục đích làm tắc nghẽn mạng hoặc khiến máy chủ hoặc dịch vụ không thể truy cập được.
* Tấn công chiếm quyền điều khiển (APT): Gói tin APT thường được sử dụng để gửi mã độc hoặc các payload khác đến máy tính của nạn nhân.
* Tấn công cài đặt phần mềm gián điệp (spyware): Gói tin spyware thường được sử dụng để theo dõi hoạt động của nạn nhân.
* Một gói tin TCP có số lượng lớn hoặc tần suất cao đến một máy chủ web có thể là dấu hiệu của một cuộc tấn công DoS. Một gói tin UDP có địa chỉ nguồn hoặc đích lạ có thể là dấu hiệu của một cuộc tấn công từ xa. Một gói tin HTTP có nội dung đáng ngờ, chẳng hạn như mã độc, có thể là dấu hiệu của một cuộc tấn công cài đặt phần mềm gián điệp

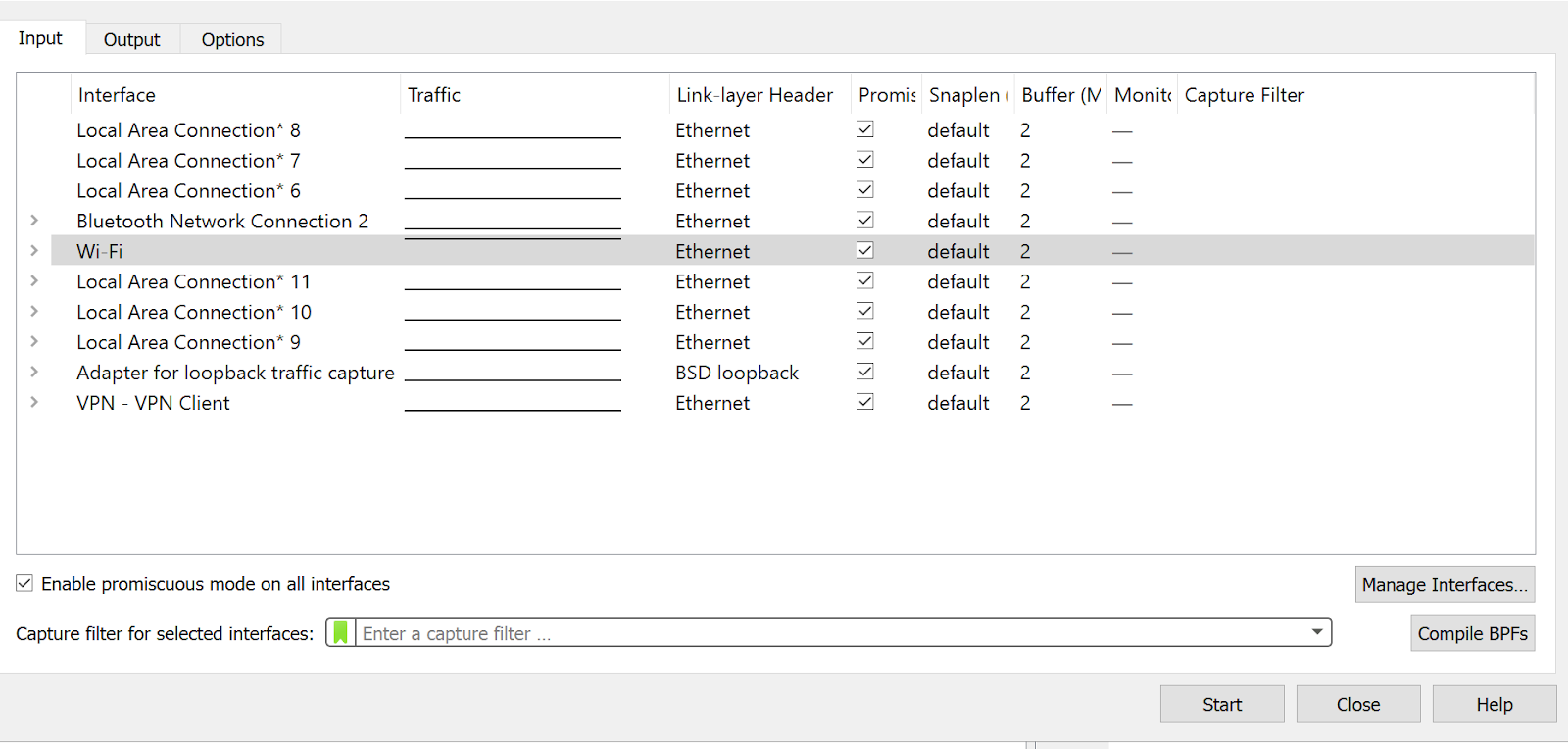
1. **Hướng dẫn sử dụng**
2. **Cách bắt các gói tin trực tiếp trong Wireshark**

Khi mở Wireshark, các giao diện mạng có trên máy sẽ được liệt kê như phía dưới. Để xem lưu lượng của 1 giao diện mạng nào đó, ta chỉ cần kích đúp vào đó, lập tức lưu lượng (các gói tin) đi qua giao diện đó sẽ được hiển thị.

Bắt gói tin trong mạng Wifi:

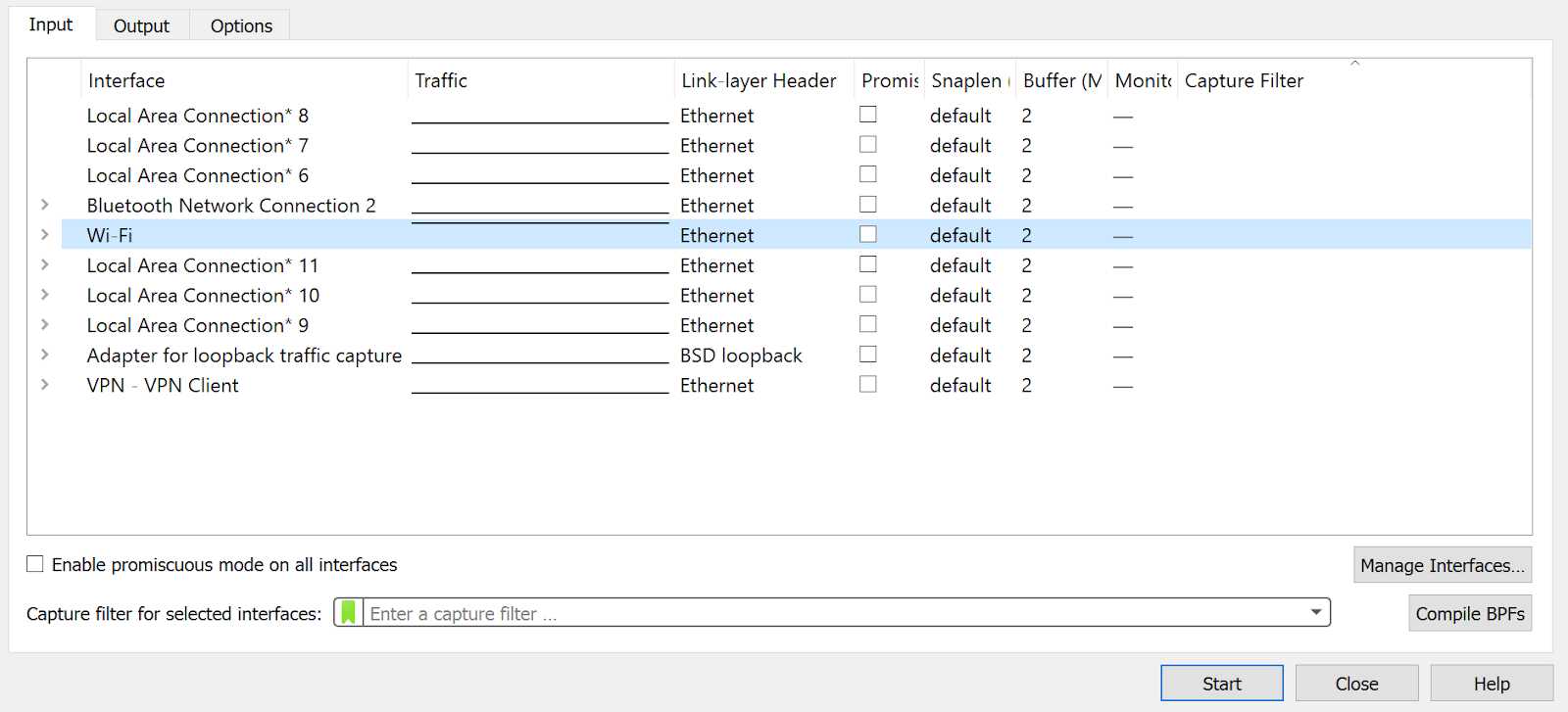
Lưu lượng các gói tin đi qua Wifi sẽ hiển thị như sau:

Click vào nút “**Stop**” màu đỏ (ở góc trên bên trái của cửa sổ hoặc chọn “Capture > Stop”) nếu muốn dừng việc capture lại.

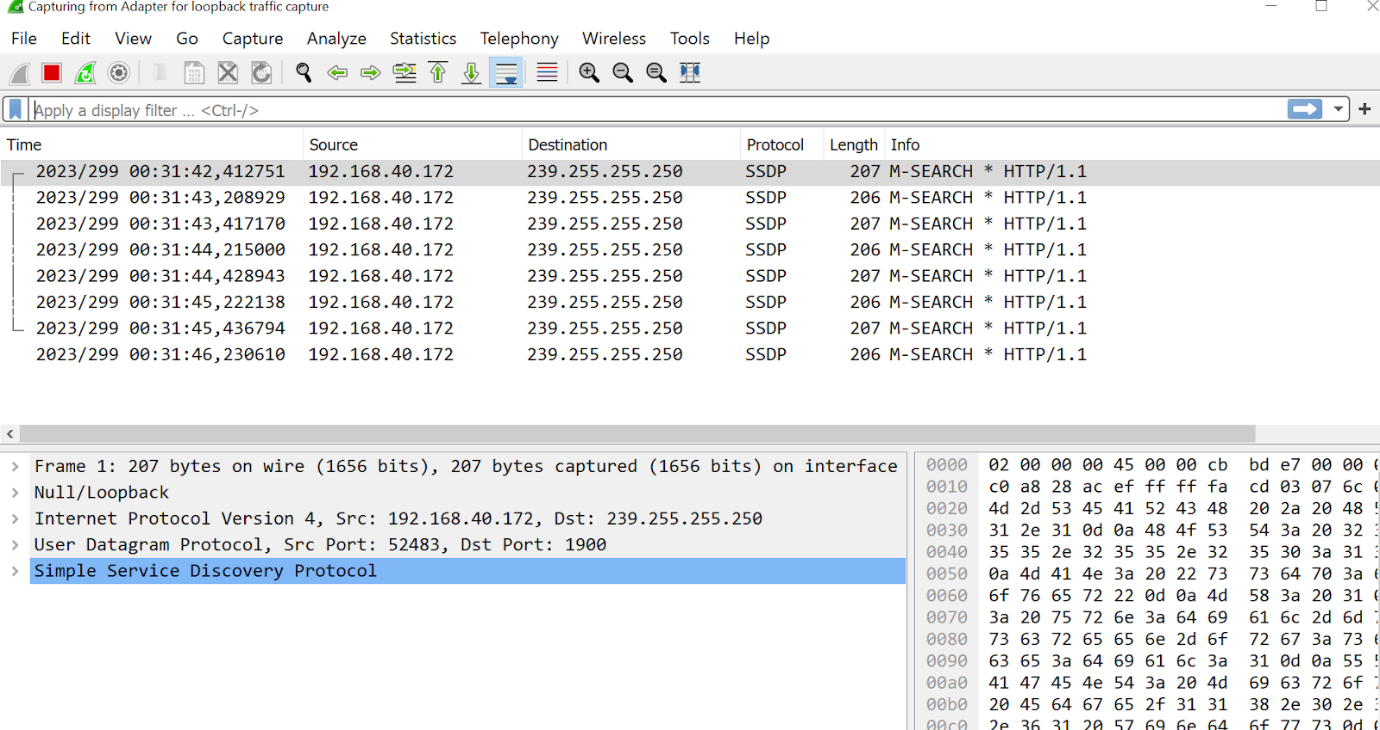
* ****Sau khi bắt được các gói tin trong mạng wifi chúng ta kiểm tra các gói mạng khác bằng cách chọn **Capture → Options**

Khi thấy “Enable promiscuous mode on all interfaces” nằm góc trái phía dưới,  chúng ta bỏ tick để chạy các gói mạng khác vì nếu vẫn để

Promiscuous chạy ở chế độ mặc định thì chúng ta sẽ thấy được tất cả các gói khác trên mạng thay vì chỉ thấy các gói được gửi tới bộ điều hợp mạng.

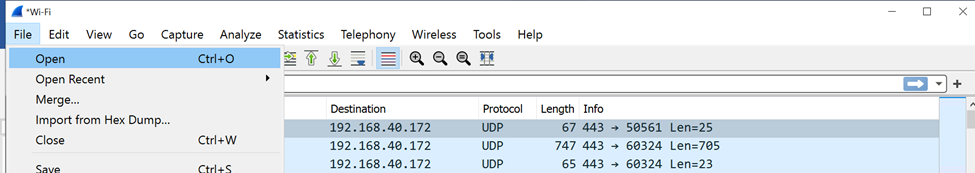
****

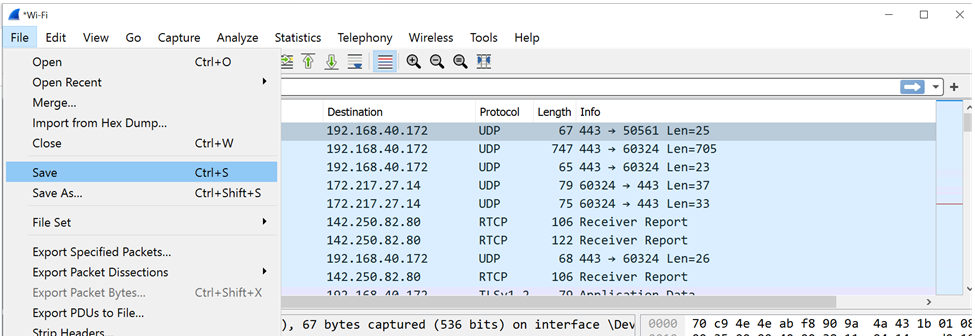
* Các gói tin trong Adapter for lookback traffic capture

****

1. **Cách lưu và mở gói tin trong Wireshark**

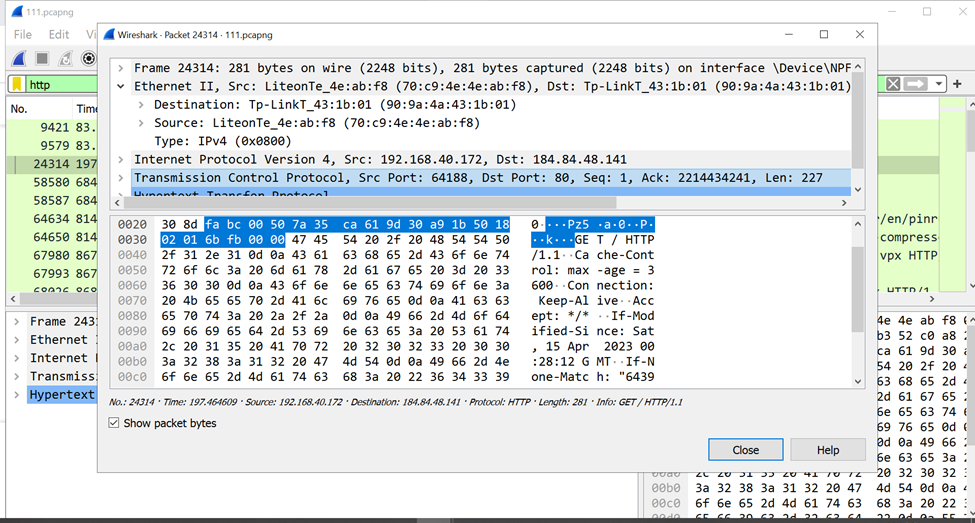
Cách mở: Chọn File > Open sau đó tìm đến đường dẫn của file cần mở



Cách lưu: Chọn File > Save. Sau đó là chọn đường dẫn để lưu trữ file rồi đặt tên cho file capture, chọn định dạng để lưu.

1. **Cách xem các gói tin trong Wireshark**

Khi đã bắt một số gói tin hoặc bạn đã mở tệp capture đã lưu trước đó, bạn có thể xem các gói được hiển thị trong Packet List bằng cách chỉ cần nhấn đúp vào một gói trong Packet List, thao tác này sẽ hiển thị gói đã chọn trong Packet Details và Packet Bytes. Sau đó, bạn có thể mở rộng bất kỳ phần nào của Packet Details để xem thông tin chi tiết về từng giao thức trong mỗi gói. Nhấp vào một mục trong Packet Details sẽ làm nổi bật các byte tương ứng trong chế độ xem byte. Ví dụ về gói HTTP được chọn sẽ hiển thị trong hình.



1. **Cách lọc các gói tin trong Wireshark**

Wireshark có hai kiểu lọc là: Capture Filters và Display Filters .

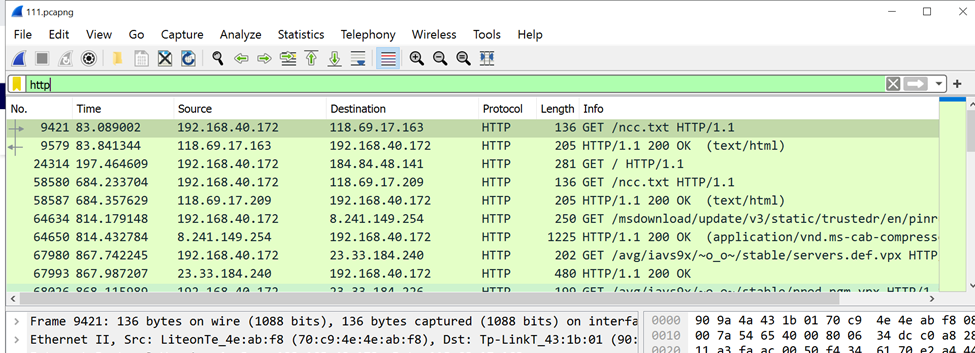
Capture Filter được sử dụng để lọc khi bắt gói tin từ các hoạt động mạng

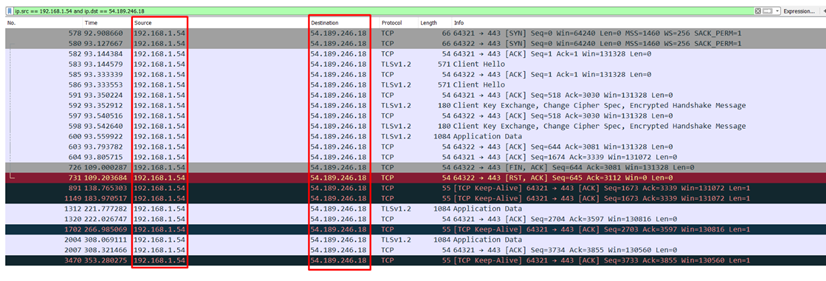
Display Filters cho phép bạn tập trung vào các gói tin mà bạn quan tâm trong khi ẩn những gói bạn không quan tâm. Chúng cho phép bạn chỉ hiển thị các gói dựa trên:

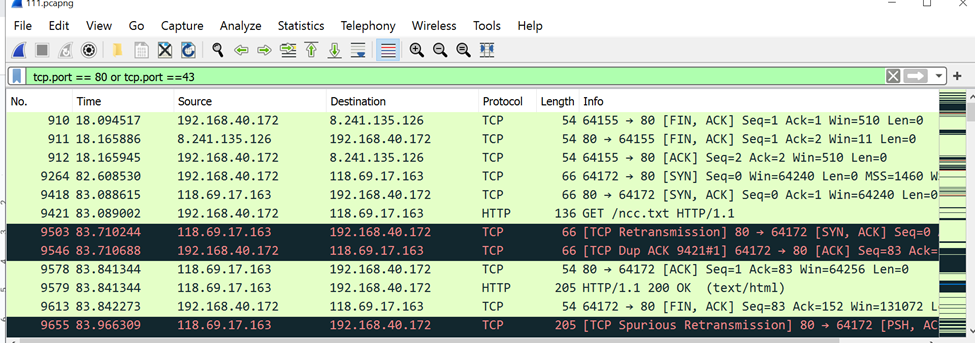
* Giao thức
* Sự hiện diện của một trường (The presence of a field)
* Giá trị của các trường (The values of fields)
* So sánh giữa các trường (A comparison between fields) … và nhiều hơn nữa

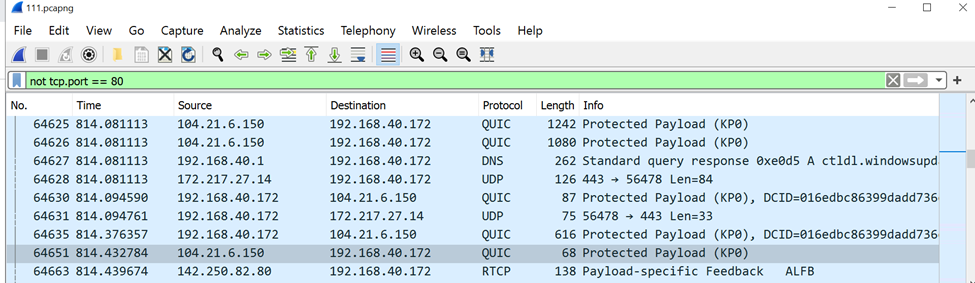
Để chỉ hiển thị các gói tin chứa một giao thức cụ thể, hãy nhập tên giao thức đó vào thanh công cụ display filter của cửa sổ Wireshark và nhấn enter để áp dụng bộ lọc.

Dưới đây là một số ví dụ về những gì sẽ xảy ra khi bạn nhập vào thanh công cụ display filter.

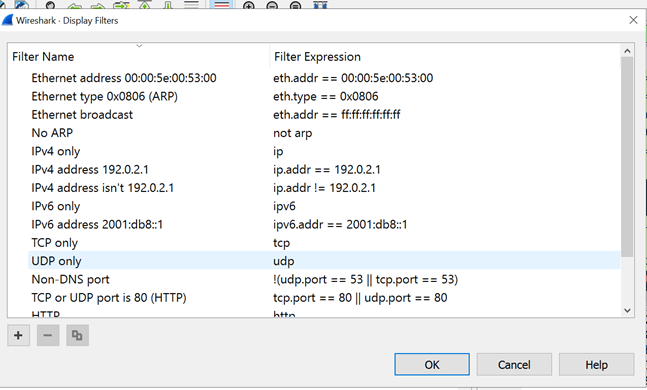
* Hiển thị các gói có phương thức HTTP
* Chỉ xem các gói có IP nguồn là 192.168.1.54 và IP đích là 54.189.246.18



* Xem các gói có TCP port là 80 hoặc TCP port là 43
* Chỉ xem các gói không sử dụng cổng 80



Ngoài ra, ta cũng có thể nhấp vào Analyze > Display Filters để tiến hành chọn bộ lọc phù hợp nhất trong số các bộ lọc mặc định mà Wireshark có và ta cũng có thể thêm bộ lọc của riêng mình và lưu chúng lại để dễ dàng truy cập khi cần.



1. **Cách Color Coding trong Wireshark**

Trong máy tính của chúng ta, các gói sẽ được đánh dấu bằng nhiều màu khác nhau và thông qua điều này, Wireshark sẽ giúp người dùng xác định các loại lưu lượng khi thực hiện truy cập một cách nhanh chóng.

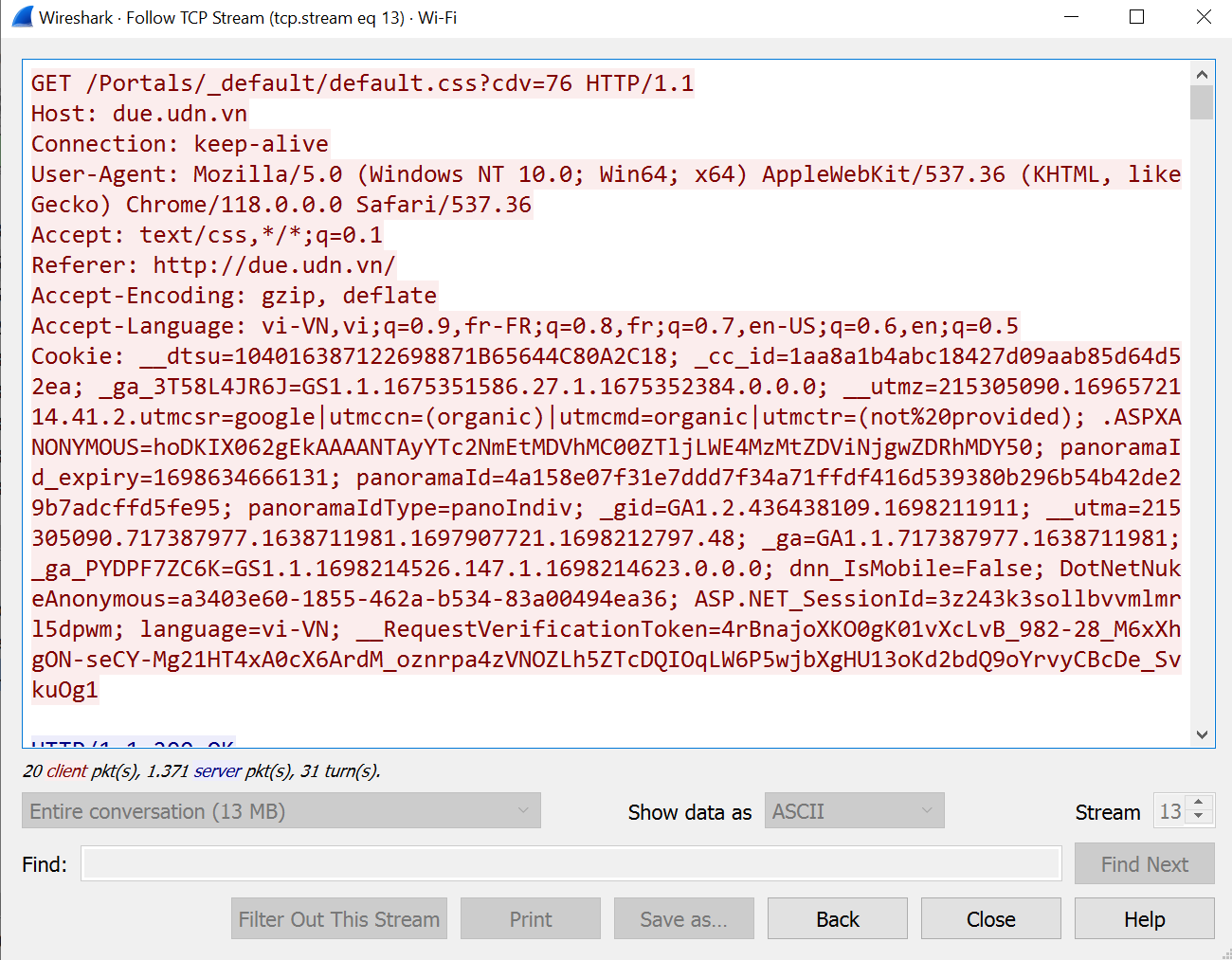
* Màu tím nhạt: lưu lượng TCP
* Màu xanh dương nhạt: lưu lượng UDP
* Màu đen: các gói có lỗi

Ta có thể nhấp vào View > Coloring Rules để xem ý nghĩa của các màu. Chúng ta hoàn toàn có thể tự điều chỉnh màu sắc theo như mong muốn của mình một cách hợp lý nhất.

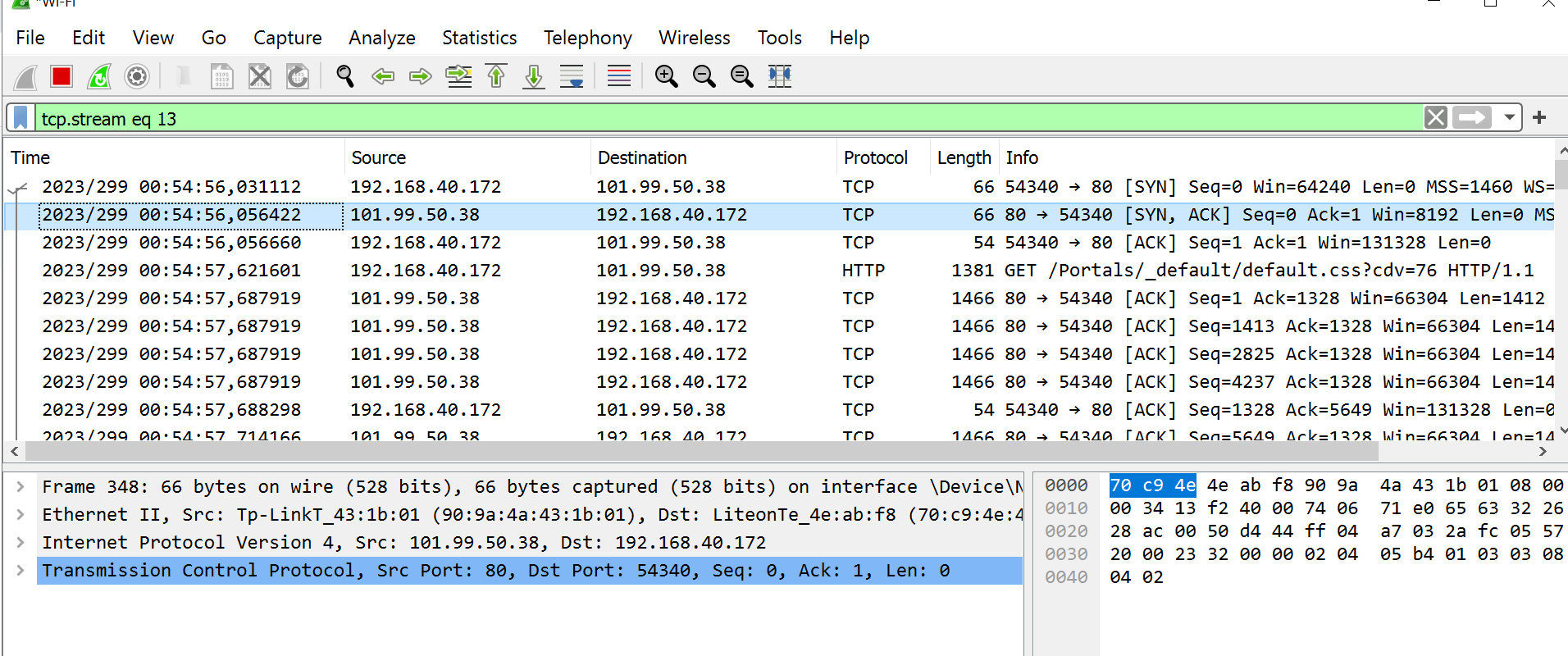


1. **Một số tính năng nâng cao của Wireshark**
2. **Following TCP Streams**

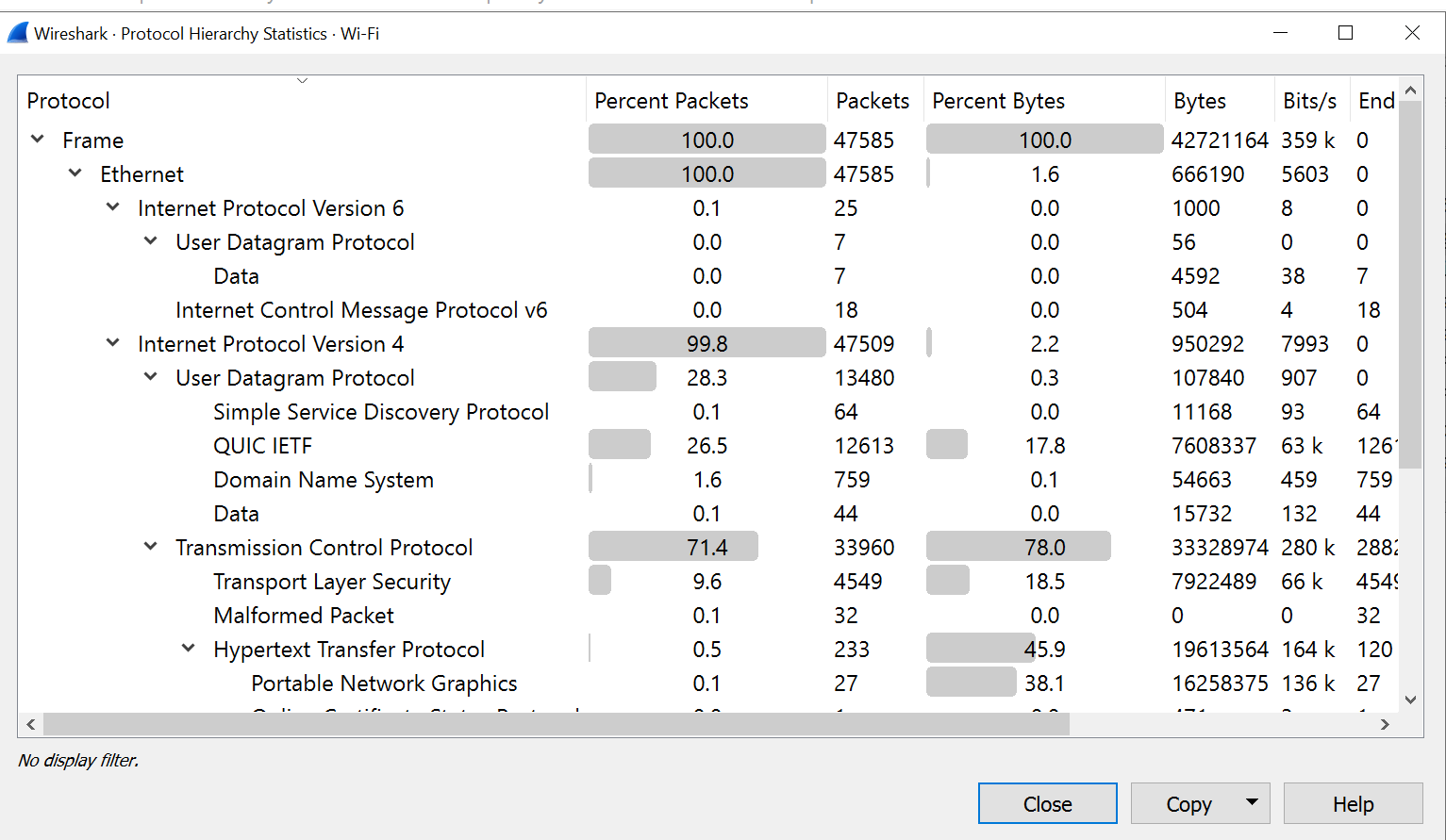
Khi nhấn chuột phải vào từng gói và chọn Follow > TCP Stream, chương trình sẽ hiển thị toàn bộ quãng thời gian giao tiếp TCP giữa máy khách và máy chủ. Bạn cũng có thể nhấp vào giao thức khác trong menu Follow để xem toàn bộ quãng thời gian giao tiếp cho những giao thức đó.



Đóng cửa sổ và bạn sẽ thấy bộ lọc đã được áp dụng tự động. Wireshark đang hiển thị các gói tạo phiên giao tiếp.

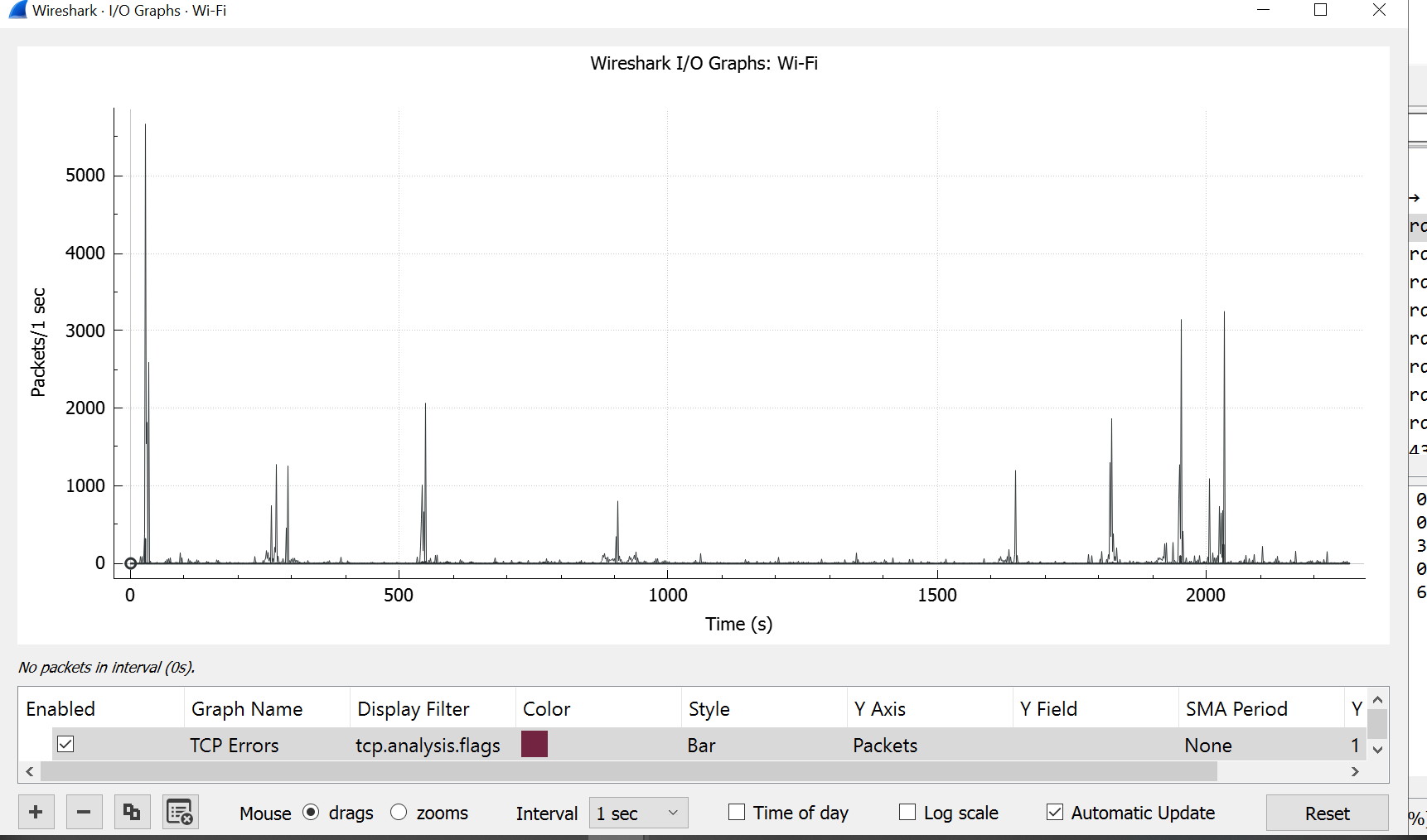


1. **Cửa sổ thống kê phân cấp giao thức**

Khi bắt được một file có kích thước lớn, chúng ta cần biết được phân bố các giao thức trong file đó, bao nhiêu phần trăm là TCP, bao nhiêu phần trăm là IP và DHCP là bao nhiêu phần trăm,…Thay vì đếm từng gói tin để thu được kết quả, chúng ta có thể sử dụng cửa sổ thống kê phân cấp giao thức Wireshark bằng cách chọn Statistics 🡪 protocol hierarchy, cửa sổ sẽ hiện ra như bên dưới.

1. **Đồ thị IO**

Nếu bạn muốn tạo một biểu diễn trực quan của các gói dữ liệu của mình, thì bạn cần mở biểu đồ IO. Chỉ cần nhấp vào Statistics chọn và chọn **I/O Graphs** . Sau đó, bạn sẽ gặp một cửa sổ đồ thị:



Chúng ta có thể thay đổi cấu hình đồ thị I/O theo dữ liệu mà mình muốn hiển thị

1. **Ưu điểm, nhược điểm của Wireshark**
2. **Ưu điểm của Wireshark**

* Wireshark hỗ trợ nhiều giao thức, giúp người dùng phân tích và theo dõi đa dạng các gói tin
* Wireshark tương thích được với nhiều nền tảng
* Cung cấp thông tin chi tiết về mỗi gói tin bao gồm : các trường dữ liệu, địa chỉ nguồn và đích, cổng và nhiều thông tin khác.
* Wireshark có sẵn trong nhiều ngôn ngữ khác nhau, giúp mở rộng sự tiếp cận của nó trên thị trường toàn cầu.

1. **Nhược điểm của Wireshark**

* Việc thu thập và phân tích lượng lớn gói tin có thể đòi hỏi tài nguyên hệ thống đáng kể, đặc biệt là khi làm việc với dữ liệu mạng lớn. Wireshark hoạt động bằng cách bắt tất cả lưu lượng mạng đi qua giao diện mạng được chọn. Điều này có thể gây nghẽn mạng, đặc biệt là trên các mạng có lưu lượng cao. Để giảm thiểu tác động này, bạn có thể sử dụng các bộ lọc để chỉ bắt các gói tin cụ thể.
* Mặc dù Wireshark có khả năng chỉnh sửa gói tin nhưng điều này mang lại nhiều rủi ro, nếu bất cẩn có thể làm thay đổi tính toàn vẹn của gói tin
* Wireshark có giao diện tương đối đơn giản nhưng vẫn khá khó hiểu đối với người mới, đòi hỏi có sự tìm hiểu cơ bản về mạng máy tính
* Trong môi trường có nguy cơ an ninh cao, việc sử dụng Wireshark có thể tạo ra rủi ro bảo mật nếu không được cấu hình và giám sát đúng cách.
* Wireshark hỗ trợ một số lượng lớn giao thức mạng, nhưng không phải tất cả. Nếu bạn cần phân tích gói tin của một giao thức mạng không được hỗ trợ, bạn có thể cần sử dụng một công cụ phân tích gói tin khác.

1. **Đánh giá, kết luận**
2. **Đánh giá**

Ta có thể thấy Wireshark là một công cụ quan trọng trong việc phân tích và giám sát mạng. Khả năng theo dõi và phân tích gói dữ liệu trên mạng giúp người dùng nắm bắt được sự hoạt động của mạng, xác định các vấn đề và gỡ rối hiệu quả.

Việc tải và sử dụng Wireshark không chỉ đơn giản mà còn mang lại nhiều lợi ích trong việc duyệt, phân tích gói dữ liệu, và theo dõi mạng. Cho dù bạn là chuyên gia hay người mới bắt đầu, công cụ này đều giúp bạn tiếp cận và tối ưu hóa hoạt động mạng một cách dễ dàng hơn.

1. **Kết luận**

Wireshark là một công cụ phân tích mạng mạnh mẽ và phổ biến trong cộng đồng mạng. Nó rất hữu ích cho các chuyên gia mạng và các nhà phân tích bảo mật để kiểm tra và theo dõi giao thông mạng. Mặc dù có một số hạn chế và yêu cầu kiến thức sâu về mạng để sử dụng hiệu quả, nhưng nó là một công cụ quan trọng trong việc quản lý và bảo vệ mạng thông tin.