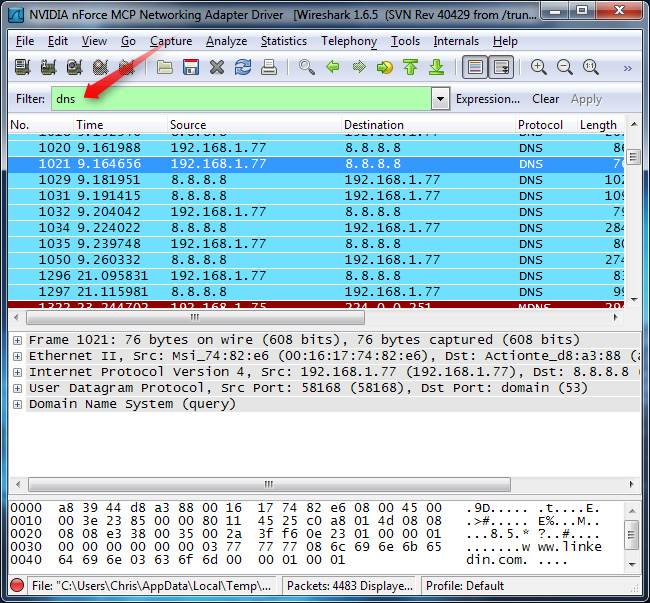
**Sử dụng Wireshark để phân tích gói dữ liệu trong hệ thống mạng**

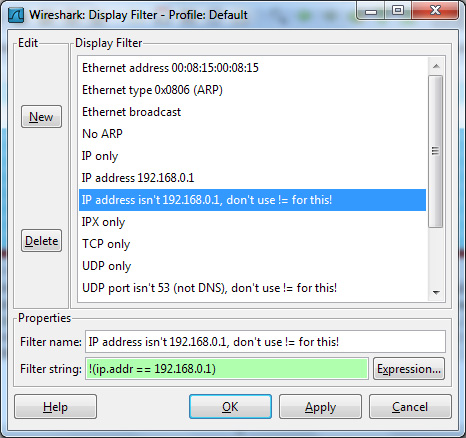
|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Quản Trị Mạng - [Wireshark](http://download.com.vn/timkiem/?query=wireshark&dir=all" \t "_blank), hay còn gọi là Ethereal, công cụ này có lẽ không quá xa lạ với phần lớn người sử dụng chúng ta, vốn được xem là 1 trong những ứng dụng phân tích dữ liệu hệ thống mạng, với khả năng theo dõi, giám sát các gói tin theo thời gian thực, hiển thị chính xác báo cáo cho người dùng qua giao diện khá đơn giản và thân thiện**. Trong bài viết dưới đây, chúng tôi sẽ giới thiệu với các bạn một số đặc điểm cơ bản cũng như cách dùng, phân tích và kiểm tra hệ thống mạng bằng **Wireshark**.  Các bạn có thể tải **Wireshark** phiên bản mới nhất tại [đây](http://download.com.vn/timkiem/?query=wireshark&dir=all" \t "_blank) hoặc trực tiếp tại [trang chủ](http://www.wireshark.org/download.html" \t "_blank). Nếu dùng **Linux**hoặc các hệ thống **UNIX**khác thì có thể tìm thấy **Wireshark**trong phần **Package** **Repositories**. Ví dụ, với **Ubuntu**thì **Wireshark**sẽ có ở trong **Ubuntu Software Center.** Tuy nhiên, các bạn cần lưu ý rằng không nên tự tiện sử dụng, vì có công ty, tổ chức hoặc doanh nghiệp không cho phép dùng Wireshark trong hệ thống mạng của họ.  **Capturing Packets:**  Sau khi cài đặt, các bạn hãy khởi động chương trình và chọn thành phần trong **Interface List** để bắt đầu hoạt động. Ví dụ, nếu muốn giám sát lưu lượng mạng qua mạng Wireless thì chọn card mạng Wifi tương ứng. Nhấn nút **Capture Options** để hiển thị thêm nhiều tùy chọn khác:  [Capturing Packets](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--02.jpg)  Ngay sau đó, chúng ta sẽ thấy các gói dữ liệu bất đầu xuất hiện, Wireshark sẽ “bắt” từng gói – package ra và vào hệ thống mạng. Nếu đang giám sát thông tin trên Wireless trong chế độ **Promiscuous**thì sẽ nhìn thấy các gói dữ liệu khác trong toàn bộ hệ thống:  <http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--03.jpg>  Nếu muốn tạm ngừng quá trình này thì các bạn nhấn nút **Stop**ở phía trên:  [nhấn Stop để ngừng hoạt động](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--04.jpg)  Tại đây, chúng ta sẽ thấy có nhiều màu sắc khác nhau, bao gồm: xanh lá cây, xanh da trời và đen. Wireshark dựa vào cơ chế này để giúp người dùng phân biệt được các loại traffic khác nhau. Ở chế độ mặc định, màu xanh lá cây là **traffic TCP**, xanh da trời đậm là **traffic DNS**, xanh da trời nhạt là **traffic UDP** và màu đen là gói**TCP**đang có vấn đề.  [các màu sắc khác nhau](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--05.jpg)  Bên cạnh đó, bạn có thể tham khảo phần hướng dẫn và ví dụ cơ bản của **Wiki Wireshark** tại [đây](http://wiki.wireshark.org/SampleCaptures" \t "_blank). Mở 1 file capture khá dễ dàng, nhấn nút **Open** và trỏ tới file gốc, người dùng còn có thể tự lưu dữ liệu capture trong Wireshark và sử dụng sau đó:  <http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--06.jpg> | |

## Filtering Packets:

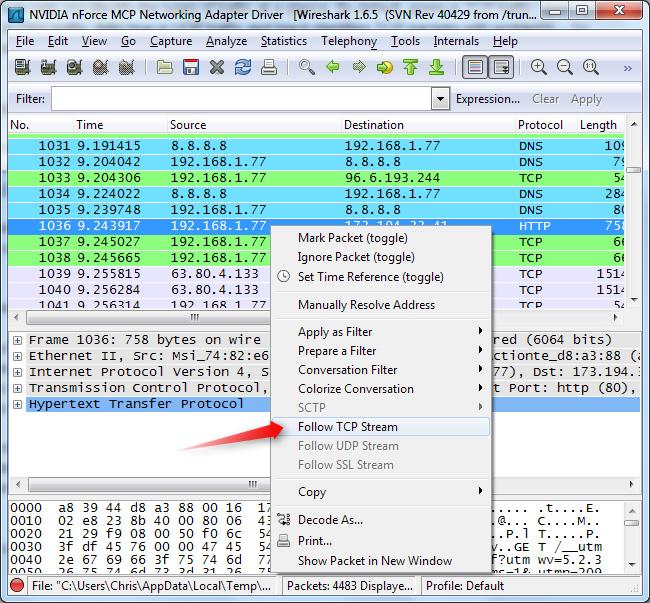
Cách cơ bản nhất để áp dụng filter là nhập thông tin vào ô **Filter**, sau đó nhấn **Apply**hoặc nhấn **Enter**. Ví dụ, nếu gõ dns thì chúng ta sẽ chỉ nhìn thấy các gói dữ liệu **DNS**. Ngay khi nhập từ khóa, **Wireshark**sẽ tự động hoàn chỉnh chuỗi thông tin này dựa vào gợi ý tương ứng.

[](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--07.jpg)

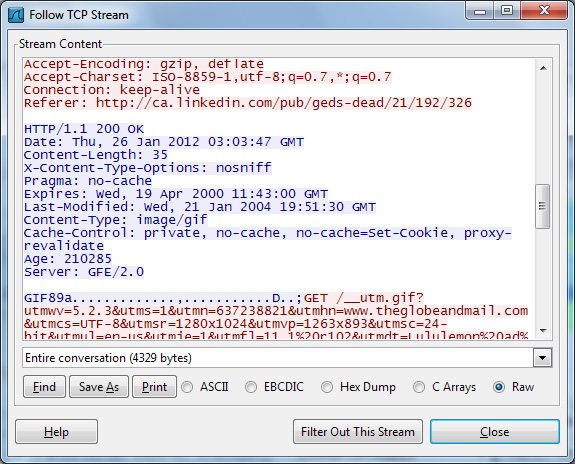
Hoặc nhấn menu **Analyze > Display Filters** để tạo filter mới:



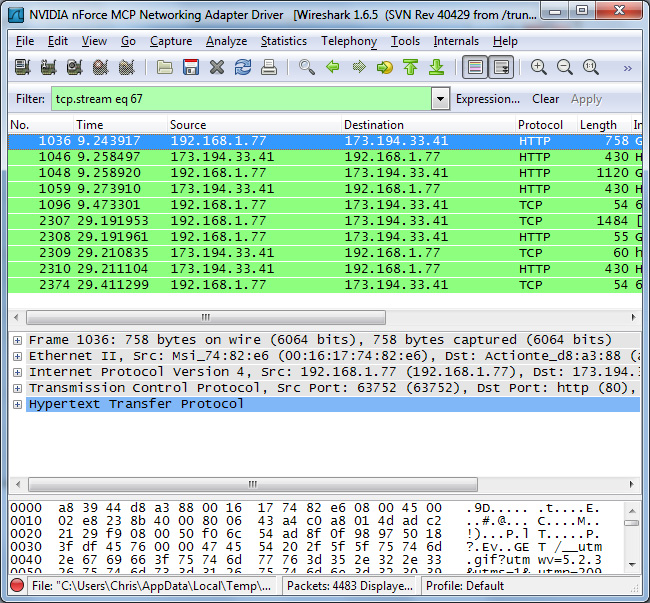
Nhấn chuột phải vào từng package và chọn **Follow TCP Stream:**

[](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--09.jpg)

Chúng ta sẽ thấy toàn bộ quãng thời gian giao tiếp giữa server và client:

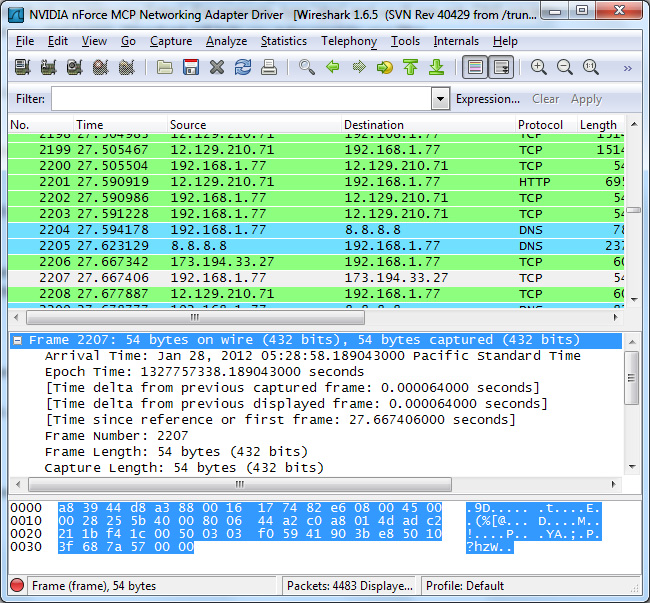


Đóng cửa sổ này lại và filter sẽ tự động được áp dụng, Wireshark tiếp tục hiển thị đầy đủ và chính xác các package có liên quan:

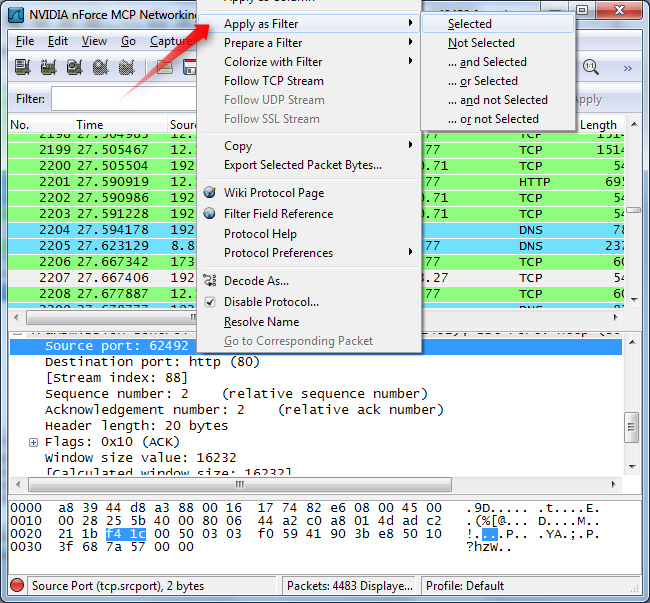
[](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--11.jpg)

## Inspecting Packets:

Nhấn và chọn 1 package bất kỳ để kiểm tra các phần thông tin cụ thể hơn:

[](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--12.jpg)

Hoặc cũng có thể trực tiếp tạo filter tại đây, nhấn chuột phải vào phần thông tin chi tiết và chọn **Apply as Filter**để áp dụng:

[](http://www.quantrimang.com.vn/photos/image/012012/31/wireshark--13.jpg)

Trên đây là một số thông tin cơ bản về cách sử dụng Wireshark để kiểm tra, phân tích dữ liệu và các gói tin trong hệ thống mạng. Chúc các bạn thành công!

Ref: quantrimang.com