HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

*****

BÀI THỰC HÀNH CHƯƠNG 1

HỌC PHẦN:
MẠNG MÁY TÍNH

Hà Nội - 2017

MỤC LỤC

BÀI THỰC HÀNH CHƯƠNG 1

1. Bài thực hành số 1

Tên bài: Cài đặt và thử nghiệm công cụ ping, ipconfig, tracert, nslookup, netstat.

❖ Chuẩn bị:

Sử dụng một máy tính chạy hệ điều hành Windows có kết nối mạng internet hoặc LAN làm môi trường thực hành.

❖ Các bước thực hiện:

a) Thử nghiệm lệnh ping

Bước 1: Chạy "Command Prompt"
Bước 2: Gõ lệnh "ping google.com"
Bước 3: Ghi nhận kết quả và phân tích - Số gói tin gửi đi: ? - Số gói tin nhận về: ? - Mất mát: ? - Trung bình thời gian gửi đi và nhận về: ?
Bước 4: Thử nghiệm thêm một số tùy chọn của lệnh ping (xem bằng "ping /?")

b) Thử nghiệm với lệnh ipconfig

Bước 1: Chạy "Command Prompt"
Bước 2: Gõ lệnh "ipconfig /all"
Bước 3: Ghi nhận kết quả và phân tích - Hệ thống có bao nhiêu giao diện mạng? - Giao diện mạng nào đang kết nối ra Internet? (giao diện có default gateway) - Địa chỉ của default gateway? - Địa chỉ IP của giao diện mạng kết nối Internet? - Địa chỉ DNS server trỏ đến?

- Có sử dụng DHCP server không? Địa chỉ của DHCP là gì?
Bước 4: Thử nghiệm thêm một số tùy chọn của lệnh ipconfig (xem bằng "*ipconfig /?"*)

c) Thử nghiệm với lệnh tracert/tracetcp/pathping

Bước 1: Chạy "Command Prompt"
Bước 2: Gõ lệnh "tracert google.com"
Bước 3: Ghi nhận kết quả và phân tích - Đường đi của gói tin qua bao nhiêu router? - Thời gian trung bình của đường đi
Bước 4: Sử dụng tracetcp google.com và ghi nhận lại kết quả như Bước 3. - tracetcp và tracert khác nhau ở đâu?
Bước 5: Sử dụng "pathping google.com" và ghi nhận lại kết quả - pathping và tracert khác nhau ở đâu?

Chú ý:

- Dấu * hiển thị trên màn hình có nghĩa bị timeout do đi quá lâu hoặc không có gói tin phản hồi.

- Do nhiều router cấm ICMP nên có thể sử dụng tracetcp thay thế lệnh tracert

https://github.com/simulatedsimian/tracetcp/releases/download/v1.0.3/tracetcp_v1.0.3.zip

- Trên HĐH Linux, ta có thể dùng bằng tiện ích traceroute với các giao thức khác nhau

d) Thử nghiệm với lệnh nslookup

Bước 1: Chạy "Command Prompt"
Bước 2: Gõ lệnh "nslookup google.com" và lệnh "nslookup 31.13.95.36"
Bước 3: Ghi nhận kết quả và phân tích - Các địa chỉ IP tương ứng của google.com? - Tên miền tương ứng của địa chỉ IP 31.13.95.36?

e) Thử nghiệm với lệnh netstat

Bước 1: Chạy "Command Prompt"
Bước 2: Gõ lệnh "netstat –a –n -o"
Bước 3: Ghi nhận kết quả và phân tích - Các loại giao thức có trong cột Proto? - Các địa chỉ IP có trong cột Local Address? - Tìm một kết nối web (có cổng 80 tại cột Foreign Address), kết nối này đang ở trạng thái nào? Đây là trang web gì (nslookup với địa chỉ IP)? - Tùy chọn a,n,o là các tùy chọn gì?
Bước 4: Sử dụng tiện ích *currports* và ghi nhận lại kết quả như Bước 3.

2. Bài thực hành số 2

Tên bài: Cài đặt và sử dụng công cụ chặn bắt gói tin Wireshark

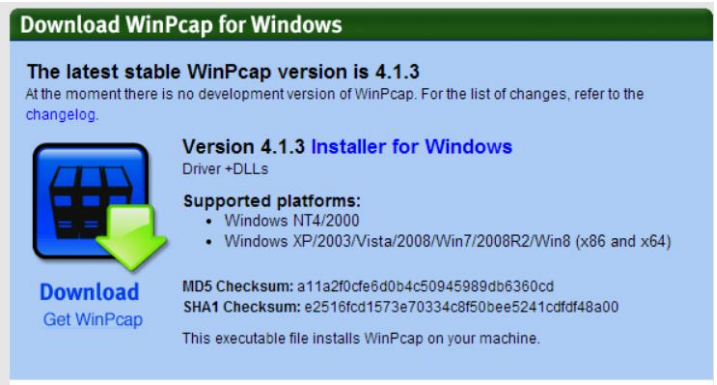
❖ Chuẩn bị:

Sử dụng một máy tính có kết nối mạng internet hoặc LAN để tiến hành bắt gói tin trên máy tính cài đặt hệ điều hành Windows

❖ Các bước thực hiện:

Bước 1: Cài đặt winpcap

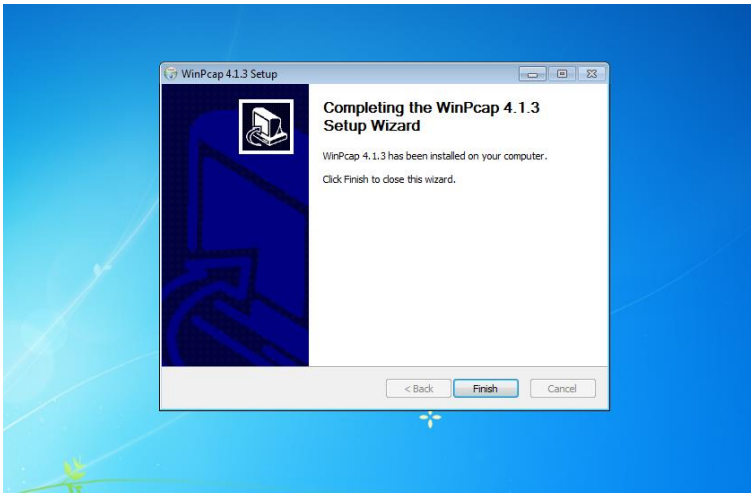
Cũng như tcpdump và winpcap, wireshark muốn hoạt động được cần có thư viện winpcap hỗ trợ việc chặn bắt và xem nội dung gói tin



Download winpcap bản mới nhất trên trang http://www.winpcap.org/. Ở trong bài này chúng ta sẽ dùng bản winpcap 4.1.3

Hình 1: Download winpcap 4.1.3 cho Windows

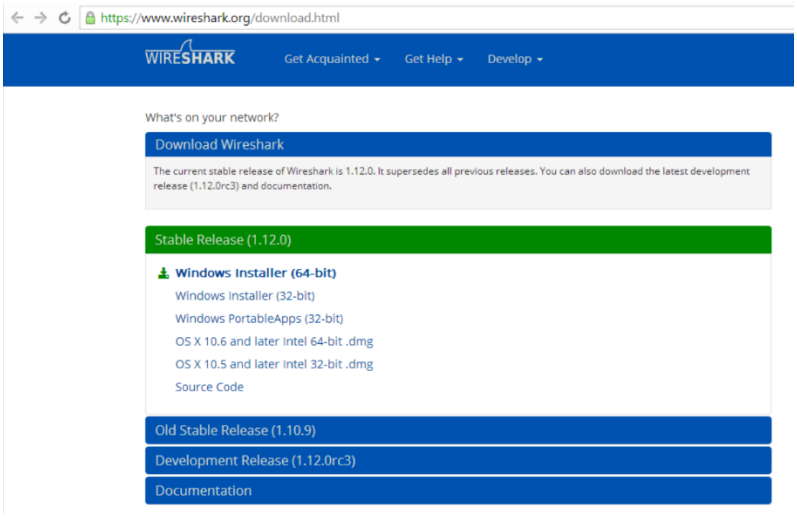
Sau khi download tiến hành cài đặt winpcap



Hình 2: Cài đặt winpcap thành công

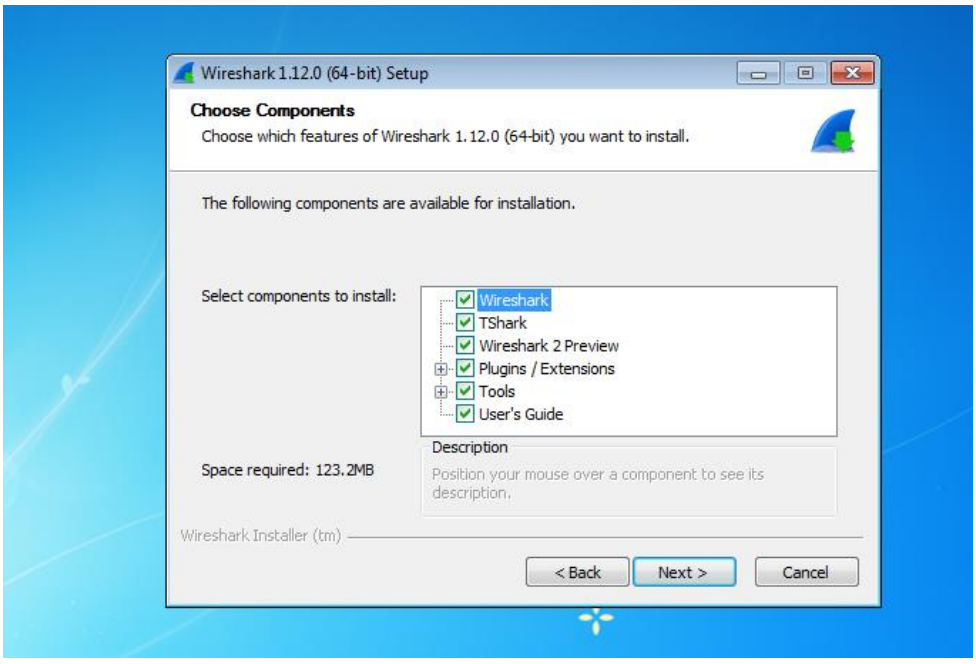
Bước 2: Cài đặt Wireshark

Download và xem thông tin liên quan đến wireshark thông qua trang https://www.wireshark.org. Ở trong bài này chúng ta sẽ sử dụng bản wireshark 1.12.0 cho Windows

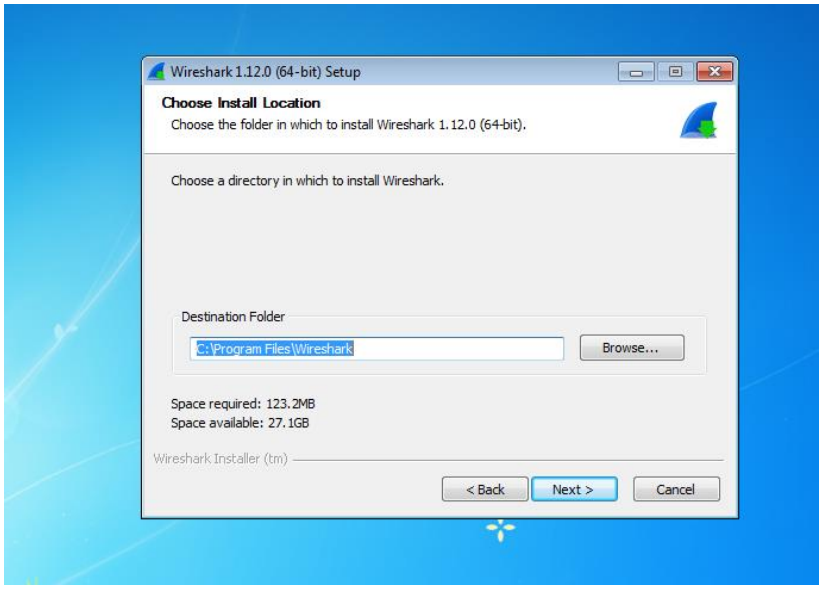


Hình 3: Download wireshark trên trang www.wireshark.org

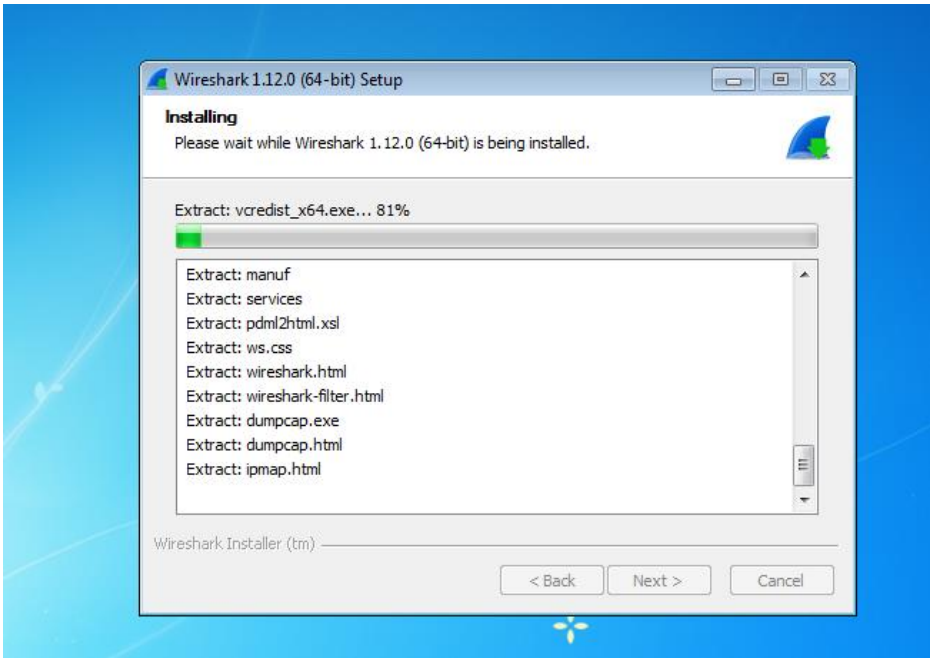
Sau khi download thành công tiến hành cài đặt bằng việc click vào biểu tượng WireShark



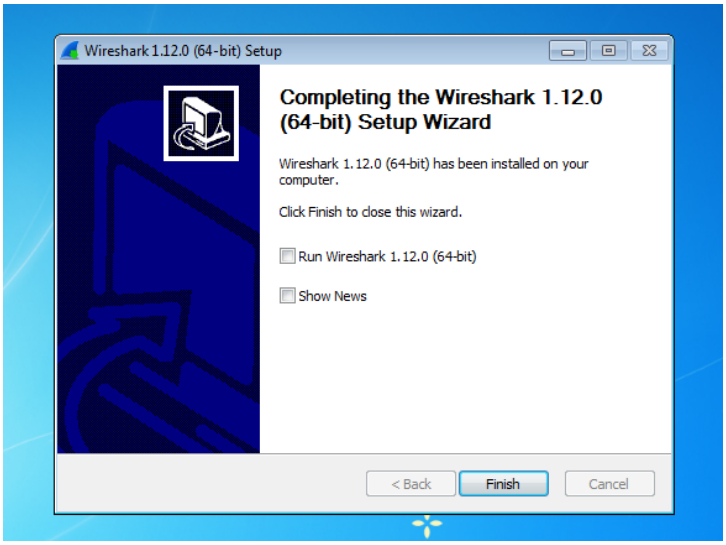
Hình 4: Lựa chọn các component khi cài đặt



Hình 5: Lựa chọn đường dẫn để cài đặt



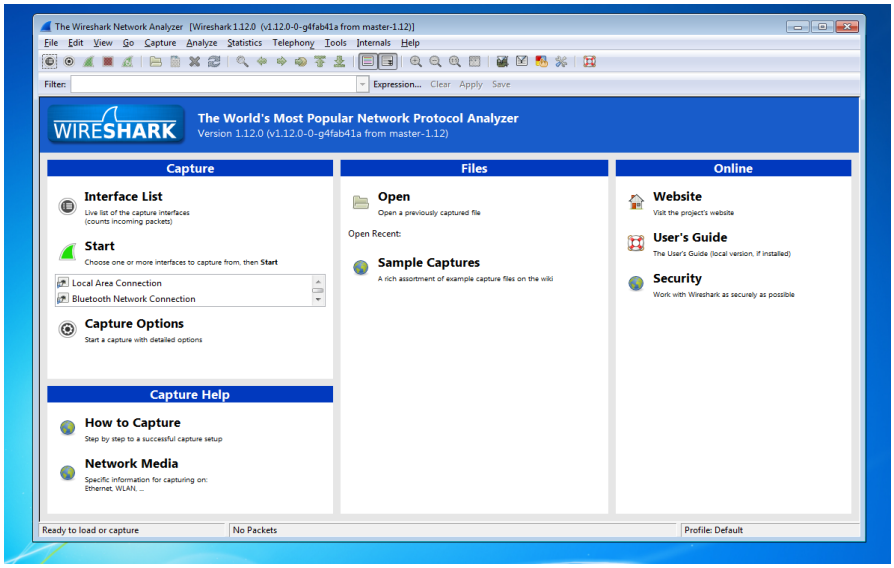
Hình 6: Install wireshark



Hình 7: Cài đặt xong wireshark

Bước 3: Sử dụng wireshark

Sau khi cài đặt thành công winpcap và wireshark chúng ta có thể sử dụng nó để chặn bắt gói tin. Wireshark là môt công cụ mạnh mẽ hỗ trợ việc chặn bắt gói tin bằng giao diện đồ họa

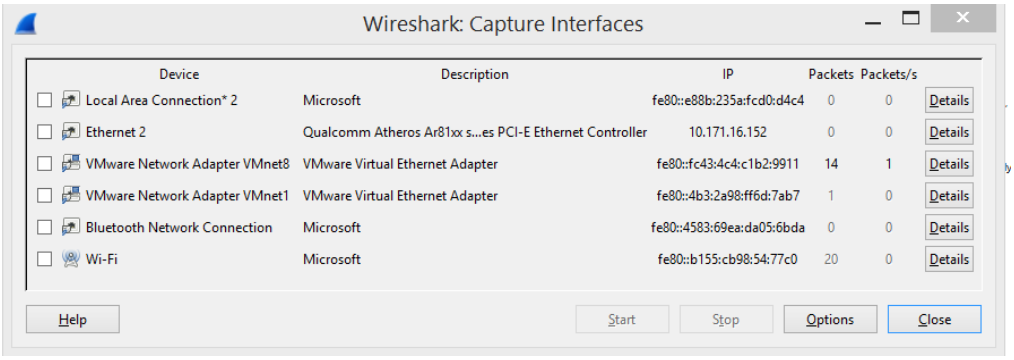


Hình 8: Giao diện chính của wireshark

Ở đây chúng ta sẽ học sử dụng một số chức năng chính của nó

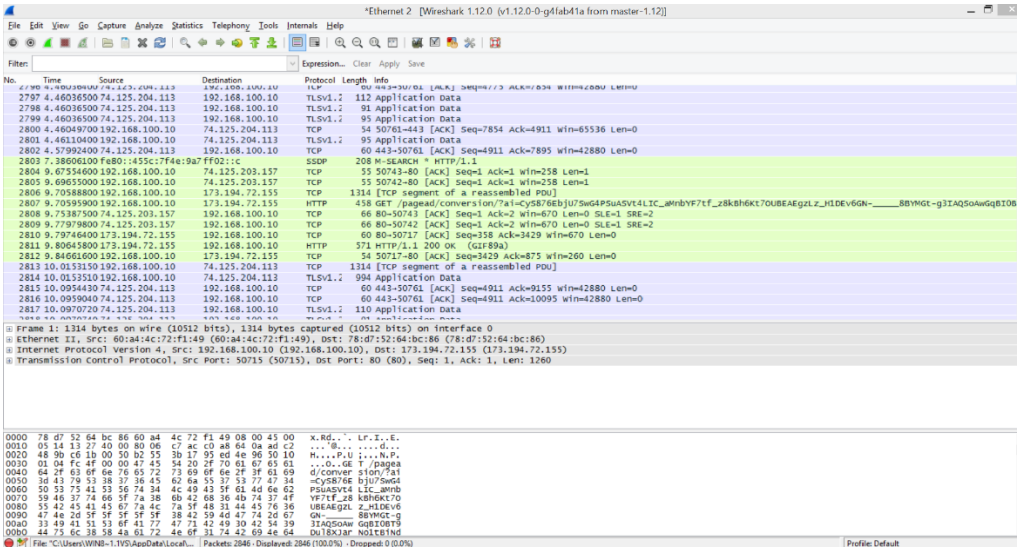
Xem và lựa chọn interface để capture:

- Click vào dòng Interface List ở màn hình chính
- Click vào capture trên thanh công cụ và chọn interface…
- Nhấm tổ hợp phím ctrl + i



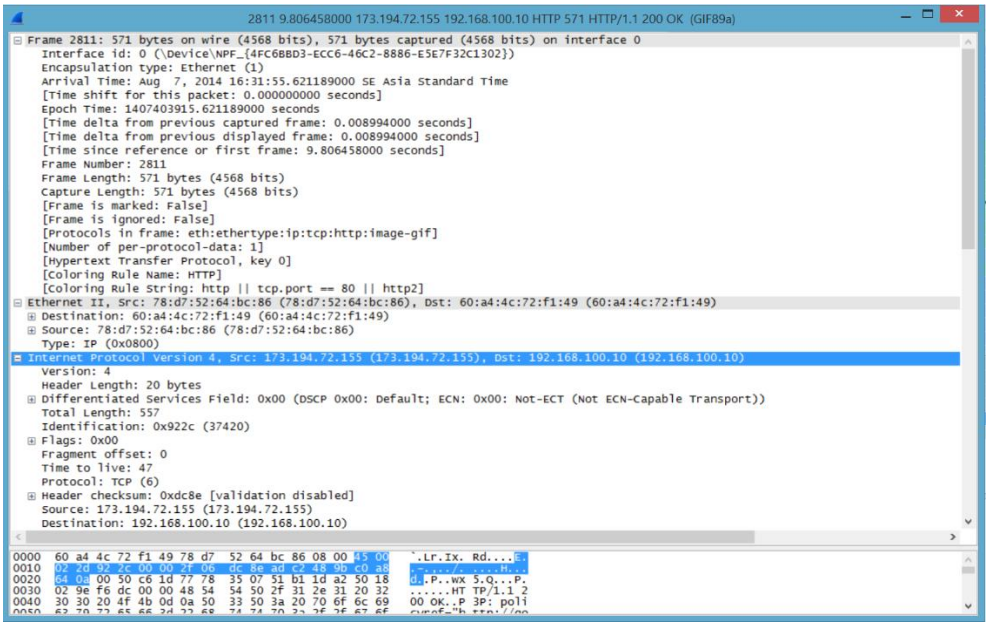
Hình 9: Giao diện hiển thị interface

Sau khi xem interface chúng ta có thể tiến hành chặn bắt gói tin qua interface đó bằng việc chọn interface và nhấn nút Start bắt đầu capture gói tin



Hình 10: Hiển thị các gói tín bắt được trên card ethernet 2

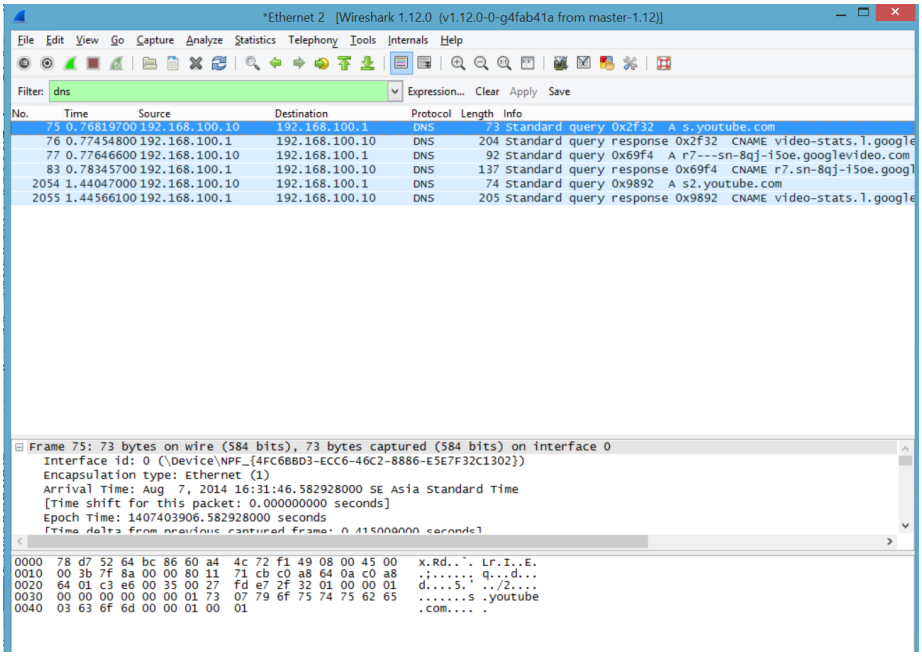
Wireshark hỗ trợ nhiều tính năng nổi bật cho phép bạn xem chi tiết nội dung từng gói tin bằng việc click 2 lần vào gói tin muốn xem nội dung



Hình 11: Xem chi tiết các gói tin

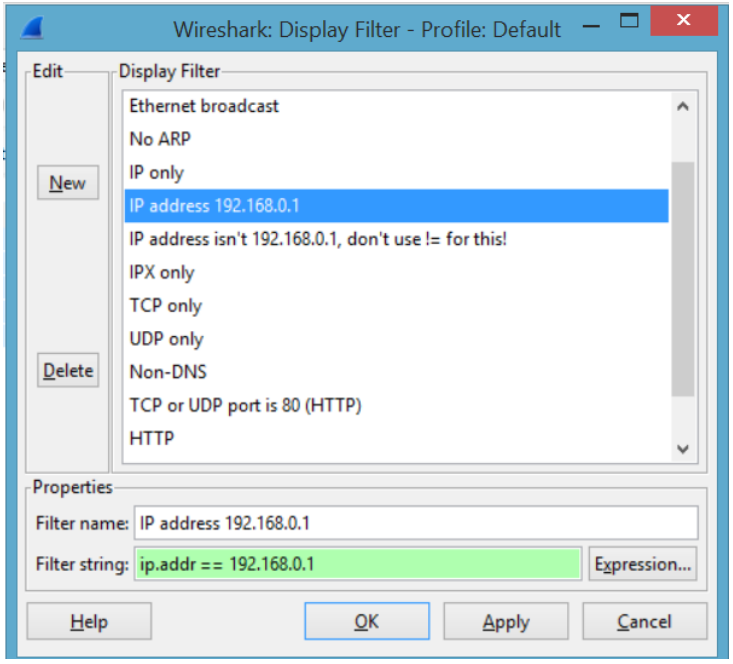
Do số lượng gói tin rất lớn mà không phải gói tin cũng cần thiết hoặc đơn giản bạn chỉ muốn xem một vài gói tin nào đó. Wireshark cung cấp chức năng filter.

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.



Hình 12: filter các gói tin DNS

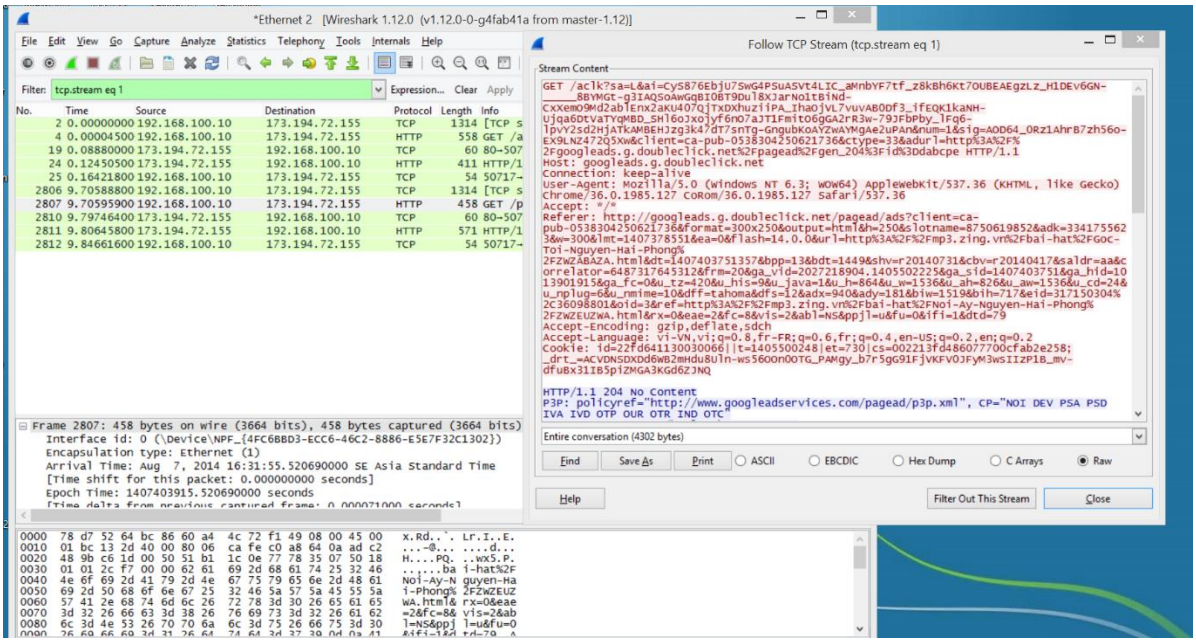
Hoặc nhấn menu Analyze > Display Filters để tạo filter mới:



Hình 13: Tạo filter mới qua giao diện Display Filters

Cách khắc nhấn chuột phải vào từng gói tin và chọn **Follow TCP Stream:**

Chúng ta sẽ thấy toàn bộ quãng thời gian giao tiếp giữa server và client, filter sẽ tự động được áp dụng, Wireshark tiếp tục hiển thị đầy đủ và chính xác các gói tin có liên quan:



Hình 14: Follow TCP Stream các gói tin

Ghi nhận phân tích kết quả

❖ Kết quả mong muốn

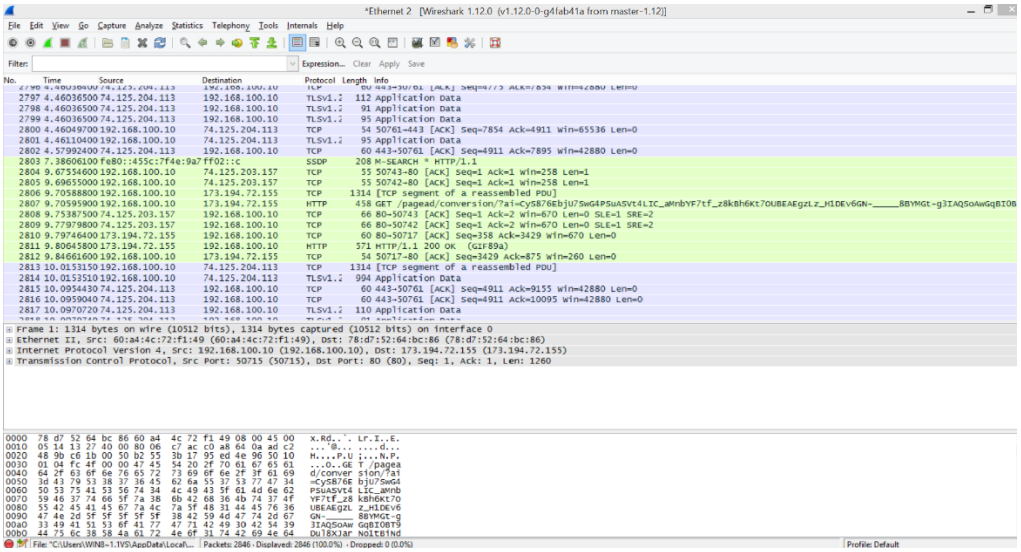
Cài đặt thành công công cụ chặn bắt gói tin wireshark và thư viện winpcap trên môi trường Windows

Sử dụng được một số chức năng của wireshark

Hiểu được cơ chế làm việc của winpcap và Wireshark

❖ Kết quả thực hiện

Sau khi cài đặt thành công wireshark, tiến hành chạy wireshark bắt các gói tin trên card mạng Ethernet 2



Filter thành công các gói tin DNS