**H**

**Ọ**

**C VI**

**Ệ**

**N CÔNG NGH**

**Ệ**

**BƯU CHÍNH VI**

**Ễ**

**N THÔNG**

**KHOA CÔNG NGH**

**Ệ**

**THÔNG TIN**

**1**

**\*\*\*\***

**\***

**BÁO CÁO BÀI THỰC HÀNH CHƯƠNG 1**

Họ và tên : Nguyễn Trường Thái

**HỌC PHẦN:**

**M**

**ẠNG MÁY TÍNH**

Mã sinh viên : B23DCCN747

**Hà N**

**ộ**

**i**

**-**

**2025**

**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.

## a) Thử nghiệm lệnh ping

|  |
| --- |
| Bước 1: Chạy “Command Prompt” |
| Bước 2: Gõ lệnh “ping google.com”  *Pinging google.com [142.250.198.110] with 32 bytes of data:*  *Reply from 142.250.198.110: bytes=32 time=26ms TTL=115*  *Reply from 142.250.198.110: bytes=32 time=29ms TTL=115*  *Reply from 142.250.198.110: bytes=32 time=27ms TTL=115*  *Reply from 142.250.198.110: bytes=32 time=27ms TTL=115*  *Ping statistics for 142.250.198.110:*  *Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),*  *Approximate round trip times in milli-seconds:*  *Minimum = 26ms, Maximum = 29ms, Average = 27ms* |
| Bước 3: Ghi nhận kết quả và phân tích   * Số gói tin gửi đi: 4 * Số gói tin nhận về: 4 - Mất mát: 0 * Trung bình thời gian gửi đi và nhận về: 27 |
| Bước 4: Thử nghiệm thêm một số tùy chọn của lệnh ping (xem bằng “ping /?”)  **Lệnh:** ping -n 10 google.com   * Kết quả: gửi 10 gói, nhận đủ 10, Average ~25 ms. * Nhận xét: mạng ổn định, không mất gói.   **Lệnh:** ping -t google.com   * Kết quả: ping liên tục, độ trễ dao động 25–30 ms. * Nhận xét: thích hợp kiểm tra ổn định đường truyền.   **Lệnh:** ping -l 200 google.com   * Kết quả: vẫn trả lời bình thường, gói tin to hơn. * Nhận xét: kiểm tra khả năng xử lý gói lớn. |

## 

## b) Thử nghiệm với lệnh ipconfig

|  |
| --- |
| Bước 1: Chạy “Command Prompt” |
| Bước 2: Gõ lệnh “ipconfig /all”  *….*  *Wireless LAN adapter Wi-Fi:*  *Connection-specific DNS Suffix . :*  *Description . . . . . . . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz*  *Physical Address. . . . . . . . . : 28-6B-35-78-22-A1*  *DHCP Enabled. . . . . . . . . . . : Yes*  *Autoconfiguration Enabled . . . . : Yes*  *Link-local IPv6 Address . . . . . : fe80::d00f:386f:a36:b4b9%12(Preferred)*  *IPv4 Address. . . . . . . . . . . : 192.168.3.109(Preferred)*  *Subnet Mask . . . . . . . . . . . : 255.255.255.0*  *Lease Obtained. . . . . . . . . . : 24 Tháng Chín 2025 8:54:37 SA*  *Lease Expires . . . . . . . . . . : 24 Tháng Chín 2025 11:54:47 SA*  *Default Gateway . . . . . . . . . : 192.168.3.3*  *DHCP Server . . . . . . . . . . . : 192.168.3.3*  *DHCPv6 IAID . . . . . . . . . . . : 170421045*  *DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-0C-33-53-28-6B-35-78-22-A1*  *DNS Servers . . . . . . . . . . . : 192.168.3.3*  *NetBIOS over Tcpip. . . . . . . . : Enabled*  *….* |
| Bước 3: Ghi nhận kết quả và phân tích   * Hệ thống có bao nhiêu giao diện mạng?   Có   * Giao diện mạng nào đang kết nối ra Internet? (giao diện có default gateway) * Wireless LAN adapter Wi-Fi * Địa chỉ của default gateway? * 192.168.3.3 * Địa chỉ IP của giao diện mạng kết nối Internet? * 192.168.3.109 * Địa chỉ DNS server trỏ đến? * 192.168.3.3   - Có sử dụng DHCP server không? Địa chỉ của DHCP là gì?  Enabled = Yes *192.168.3.3*  - Số giao diện mạng: ~10 (gồm card thật và card ảo VPN/VM/Hyper-V). - Giao diện kết nối Internet: Wireless LAN adapter Wi-Fi. - Default Gateway: 192.168.3.3 - IPv4 Address: 192.168.3.109 - DNS Server: 192.168.3.3 - DHCP: Enabled = Yes - DHCP Server: 192.168.3.3 |
| Bước 4: Thử nghiệm thêm một số tùy chọn của lệnh ipconfig (xem bằng “*ipconfig /?”*)  **ipconfig /release**   * Kết quả: Địa chỉ IPv4 trên card Wi-Fi bị xóa, không còn Default Gateway. * Nhận xét: Máy mất kết nối mạng do không còn IP.   **ipconfig /renew**   * Kết quả: Card Wi-Fi được cấp lại IP 192.168.3.109, Gateway 192.168.3.3.   Nhận xét: Lệnh này xin lại IP từ DHCP server.  **ipconfig /flushdns**   * Kết quả: Thông báo *Successfully flushed the DNS Resolver Cache.* * Nhận xét: Xóa cache DNS để tránh lỗi phân giải tên miền.   **ipconfig /displaydns**   * Kết quả: ban đầu báo *Could not display the DNS Resolver Cache.* * Sau khi truy cập web, chạy lại sẽ hiện tên miền và IP. * Nhận xét: Dùng để xem DNS cache trên máy. |

## 

## c) Thử nghiệm với lệnh tracert/tracetcp/pathping

|  |
| --- |
| Bước 1: Chạy “Command Prompt” |
| Bước 2: Gõ lệnh “tracert google.com”  *Tracing route to google.com [142.250.198.110]*  *over a maximum of 30 hops:*  *1 6 ms 3 ms 1 ms 192.168.3.3*  *2 18 ms 4 ms 1 ms 192.168.1.1*  *3 11 ms 3 ms 4 ms 100.123.0.134*  *4 \* 51 ms \* 42.112.3.42*  *5 7 ms 4 ms 4 ms 100.123.0.253*  *6 15 ms 4 ms 4 ms 42.112.4.85*  *7 8 ms 4 ms 7 ms 118.70.1.120*  *8 14 ms 3 ms \* 118.70.1.121*  *9 7 ms 8 ms 5 ms 1.53.123.85*  *10 32 ms 23 ms 23 ms 118.69.253.73*  *11 28 ms 23 ms 24 ms 74.125.32.112*  *12 31 ms 31 ms 29 ms 142.250.60.155*  *13 26 ms 23 ms 22 ms 66.249.95.129*  *14 26 ms 25 ms 23 ms nchkgb-af-in-f14.1e100.net [142.250.198.110]*  *Trace complete.* |
| Bước 3: Ghi nhận kết quả và phân tích   * Đường đi của gói tin qua bao nhiêu router? Có 14 router * Thời gian trung bình của đường đi: ~25 ms |
| Bước 4: Sử dụng tracetcp google.com và ghi nhận lại kết quả như Bước 3.  - tracetcp và tracert khác nhau ở đâu?  Lệnh tracert dùng gói ICMP để truy vết đường đi, thường bị một số router/firewall chặn nên có thể xuất hiện dấu “\*”. Trong khi đó, tracetcp dùng gói TCP SYN gửi đến một cổng dịch vụ cụ thể (như 80 hoặc 443), nhờ vậy phản ánh sát hơn đường đi thật sự của kết nối web và vượt qua được chặn ICMP. Điểm khác biệt chính là tracert kiểm tra bằng ICMP, còn tracetcp kiểm tra bằng TCP thực tế. |
| Bước 5: Sử dụng “pathping google.com” và ghi nhận lại kết quả - pathping và tracert khác nhau ở đâu?  tracert chỉ liệt kê các hop và độ trễ từng hop. pathping kết hợp cả tracert và ping: ngoài việc hiển thị đường đi, nó còn gửi nhiều gói để tính toán tỉ lệ mất gói và độ trễ trung bình tại từng router. Vì vậy, tracert nhanh và đơn giản, trong khi pathping chậm hơn nhưng cho thông tin chi tiết hơn về mất gói và chất lượng đường truyền. |

## 

## 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”  Server: UnKnown  Address: 192.168.3.3  Non-authoritative answer:  Name: google.com  Addresses: 2404:6800:4005:826::200e  142.250.197.110  Server: UnKnown  Address: 192.168.3.3  Name: edge-z-m-mini-shv-02-cgk1.facebook.com  Address: 31.13.95.36 |
| Bước 3: Ghi nhận kết quả và phân tích   * Các địa chỉ IP tương ứng của google.com? * **Các địa chỉ IP của google.com:**   + IPv6: 2404:6800:4005:826::200e   + IPv4: 142.250.197.110   → Một tên miền có thể ánh xạ nhiều địa chỉ IP khác nhau (để cân bằng tải và tối ưu tốc độ).   * Tên miền tương ứng của địa chỉ IP 31.13.95.36? * **edge-z-m-mini-shv-02-cgk1.facebook.com**. |

## 

## 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

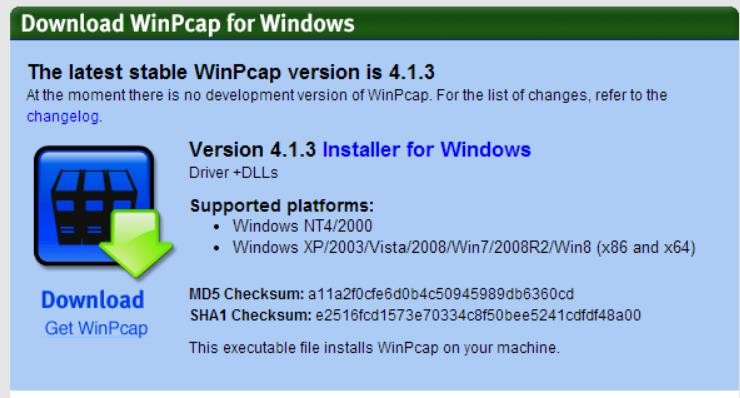
* Chuẩn bị:

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/.](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



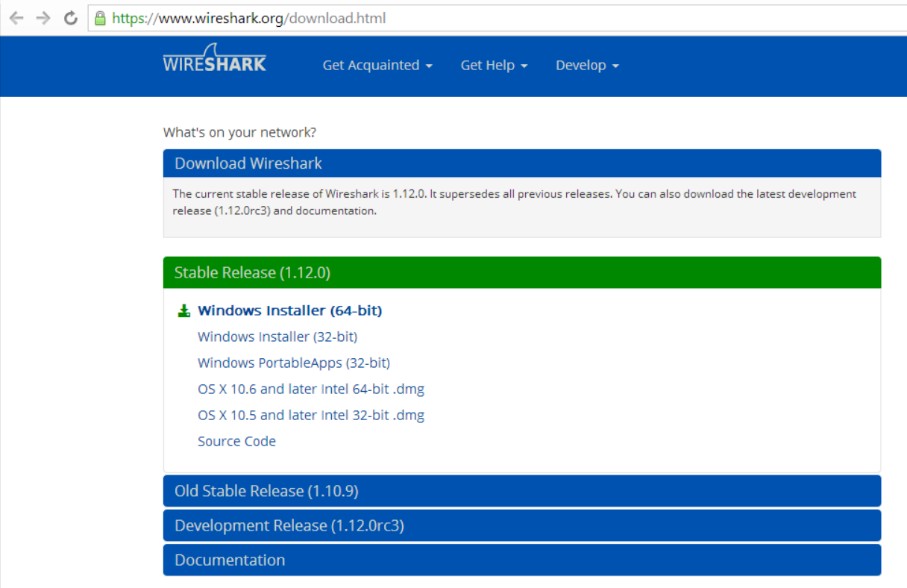
#### Hình 2: Cài đặt winpcap thành công

**Bước 2:** Cài đặt Wireshark

Download và xem thông tin liên quan đến wireshark thông qua trang

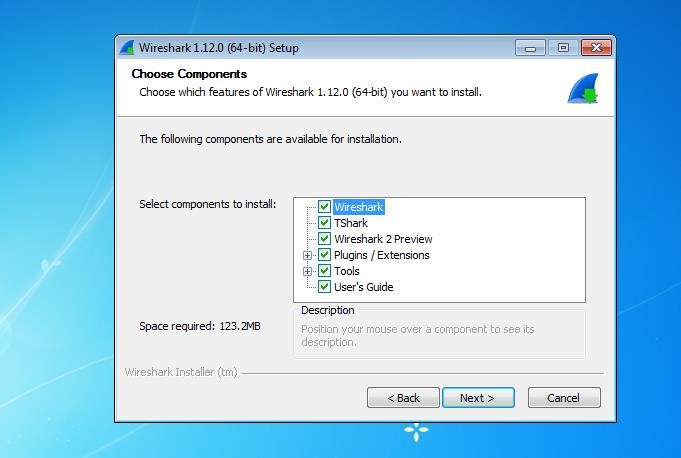
[https://www.wireshark.org.](https://www.wireshark.org/) Ở trong bài này chúng ta sẽ sử dụng bản wireshark 1.12.0 cho

Windows

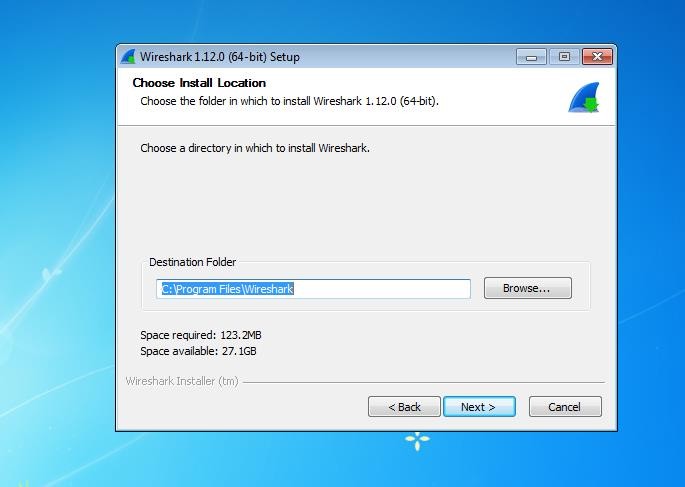


#### Hình 3: Download wireshark trên trang www.wireshark.org

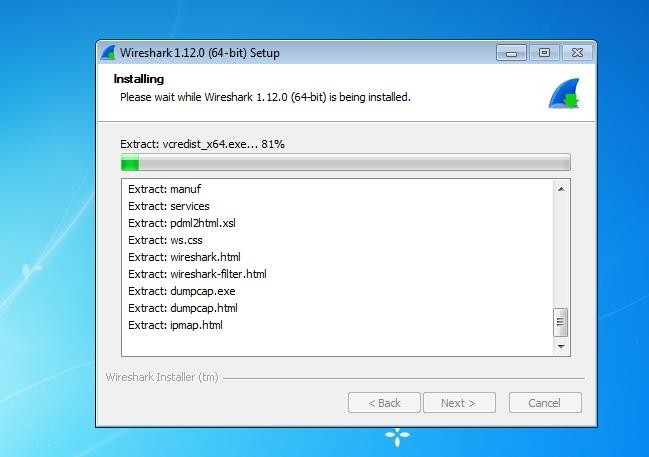
Sau khi download thành công tiến hành cài đặt bằng việc click vào biểu tượng WireShark



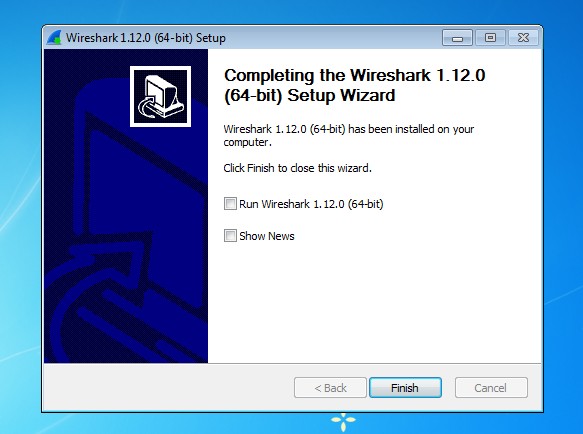
#### Hình 4: Lựa chọn các component khi cài đặt



***Hình 5: Lựa chọn đường dẫn để cài đặt***



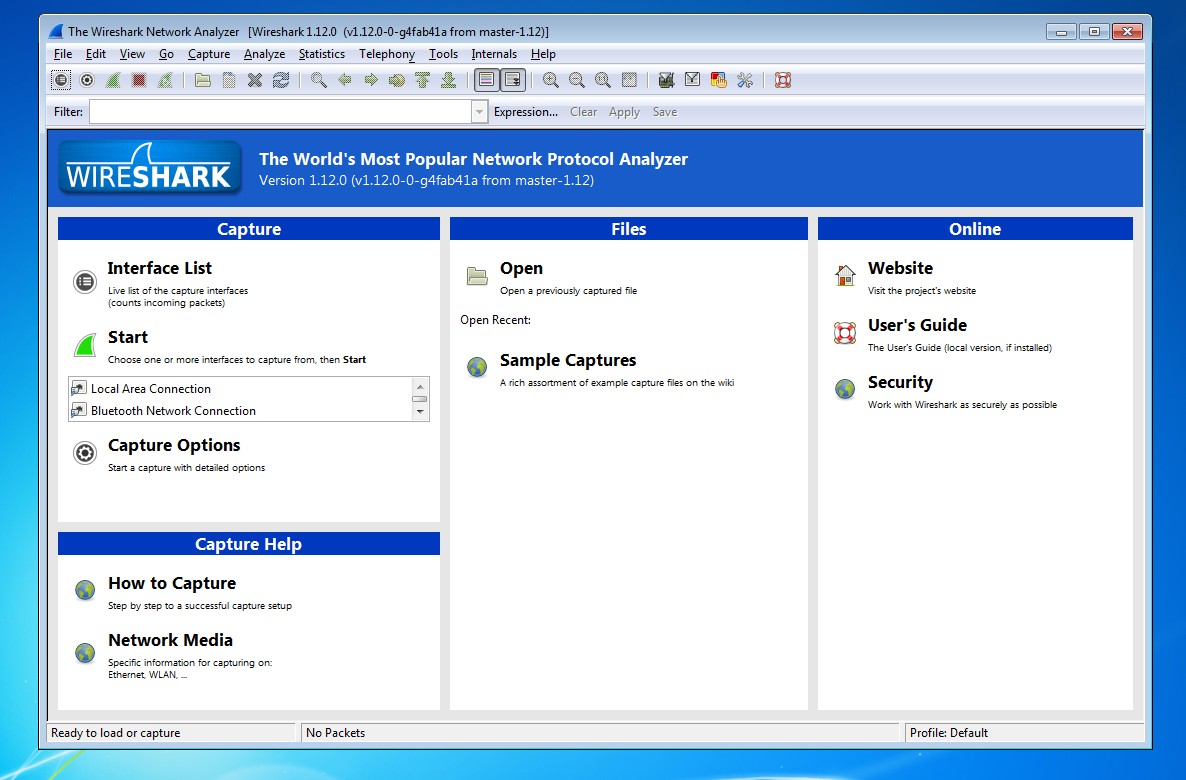
***Hình 6: Install wireshark***



#### 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

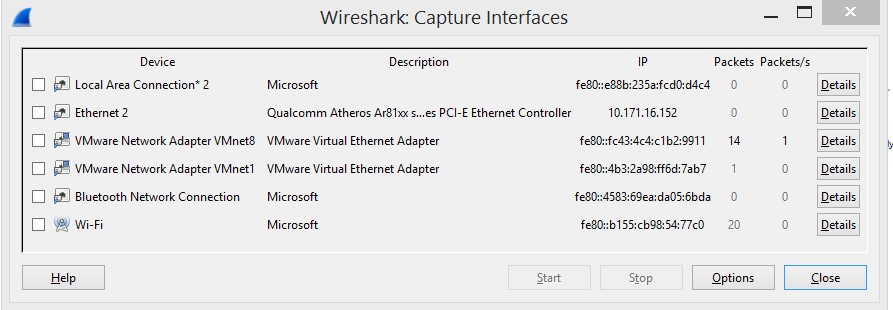


#### Hình 8: Giao diện chính của wireshark

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

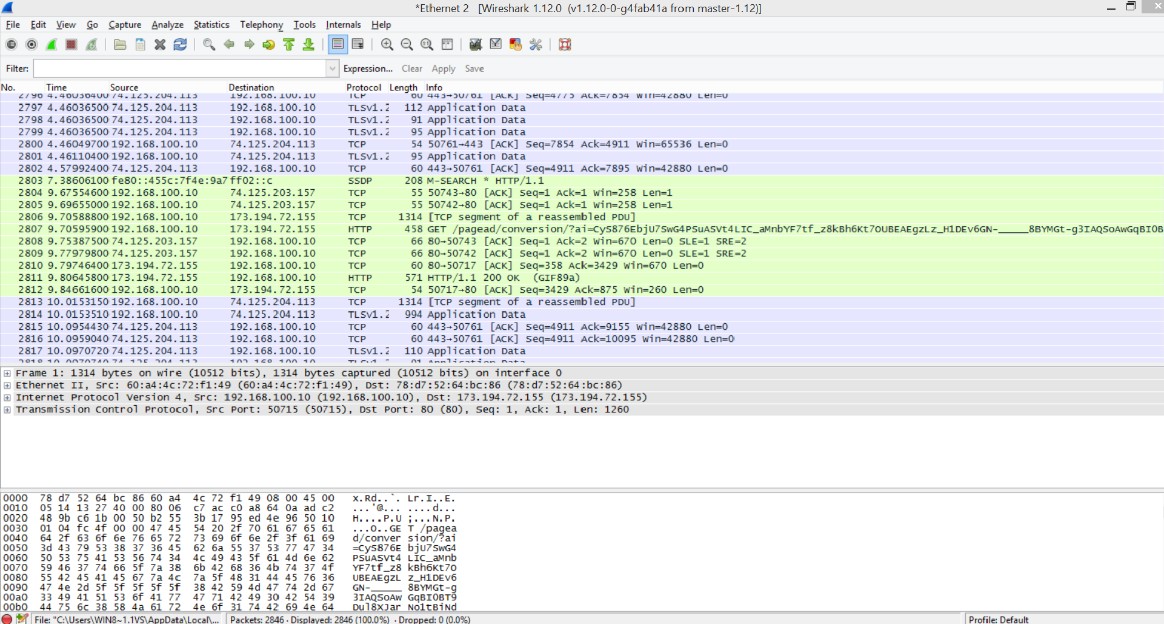
Xem và lựa chọn interface để capture:

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



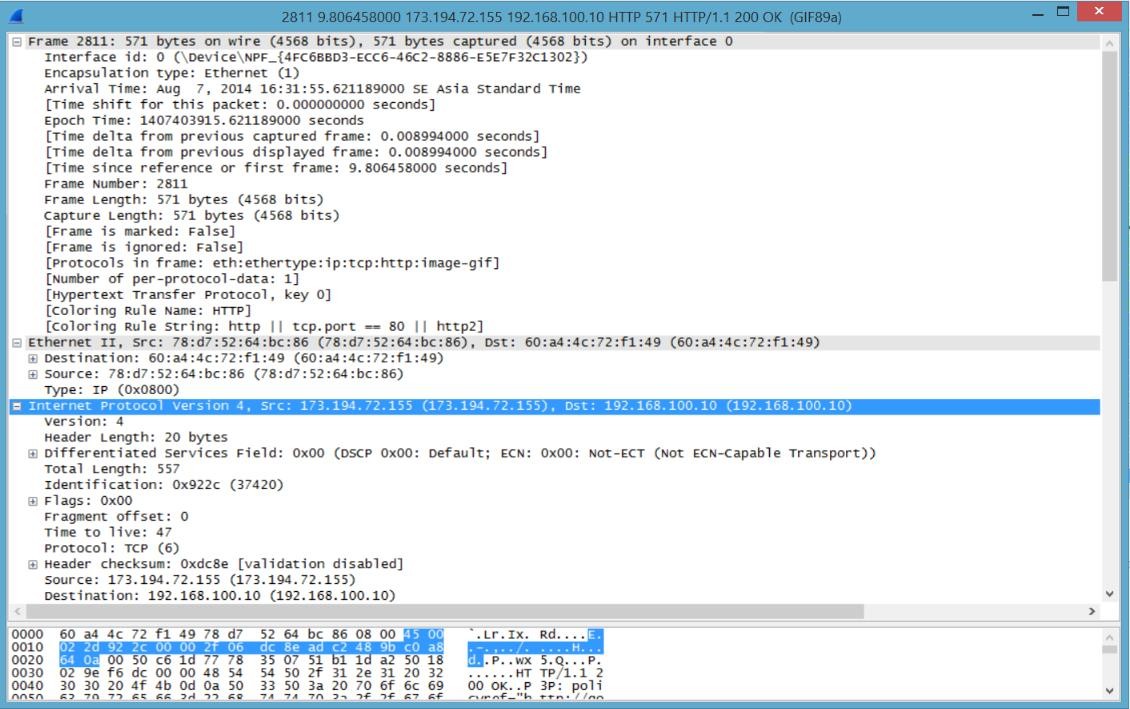
#### Hình 9: Giao diện hiển thị interface

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***

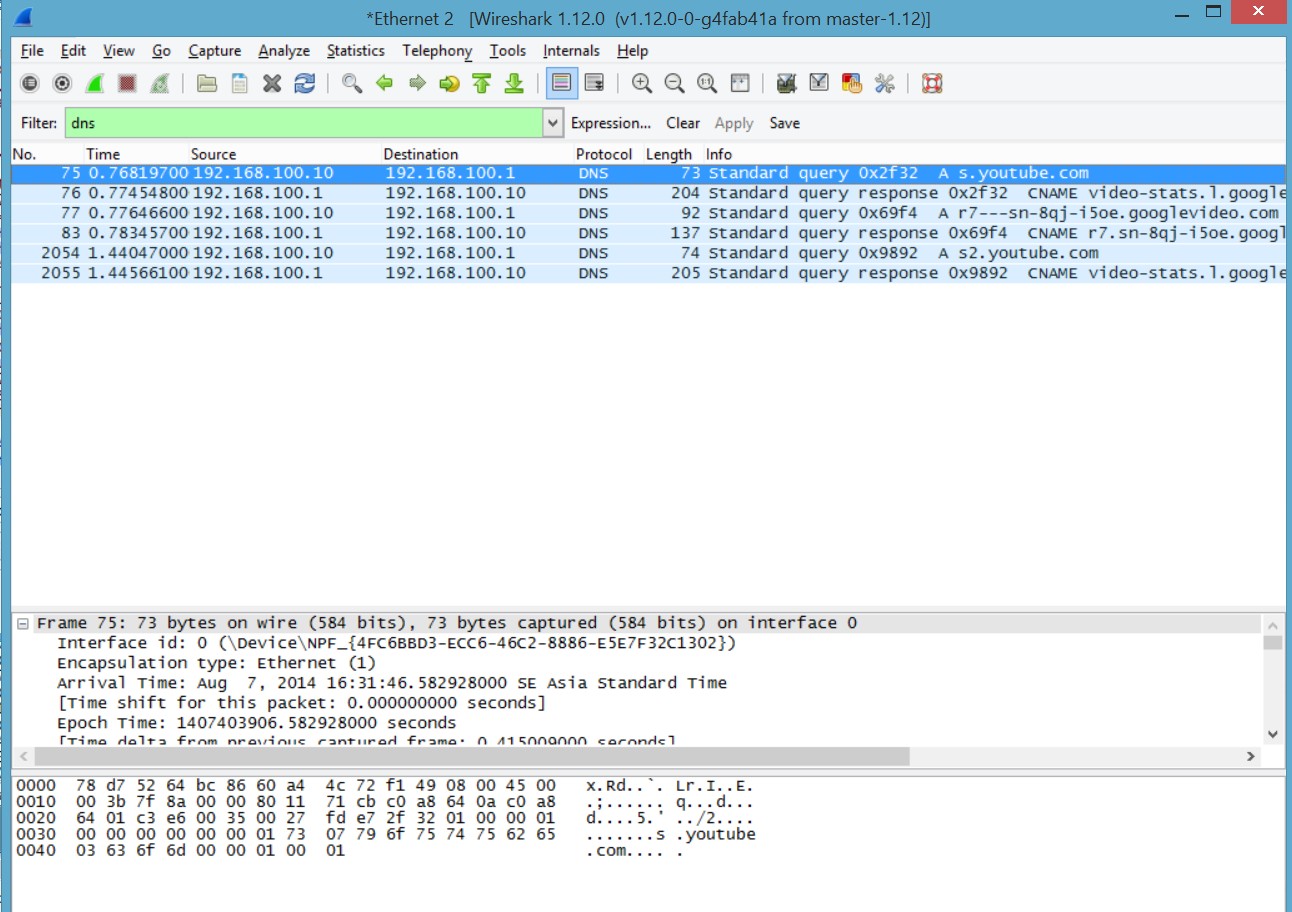
Wireshark hỗ trợ nhiều tính năng nổi bật cho phép bạn xem chi tiết nội dung từng gói tin bằng việc click 2 lần vào gói tin muốn xem nội dung



#### Hình 11: Xem chi tiết các gói tin

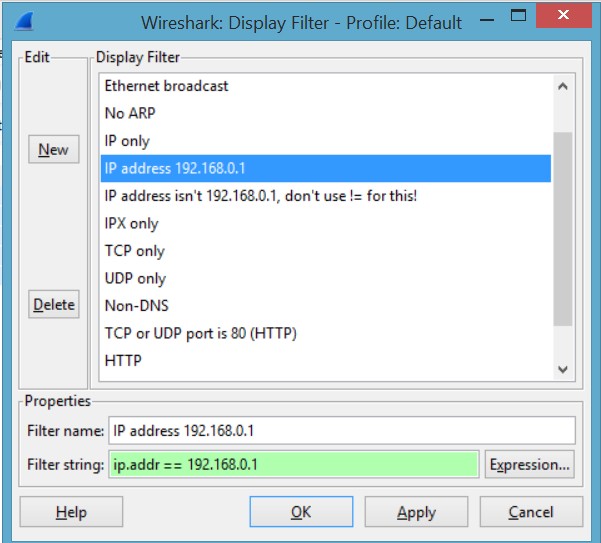
Do số lượng gói tin rất lớn mà không phải gói tin cũng cần thiết hoặc đơn giản bạn chỉ muốn xem một vài gói tin nào đó. Wireshark cung cấp chức năng filter.

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

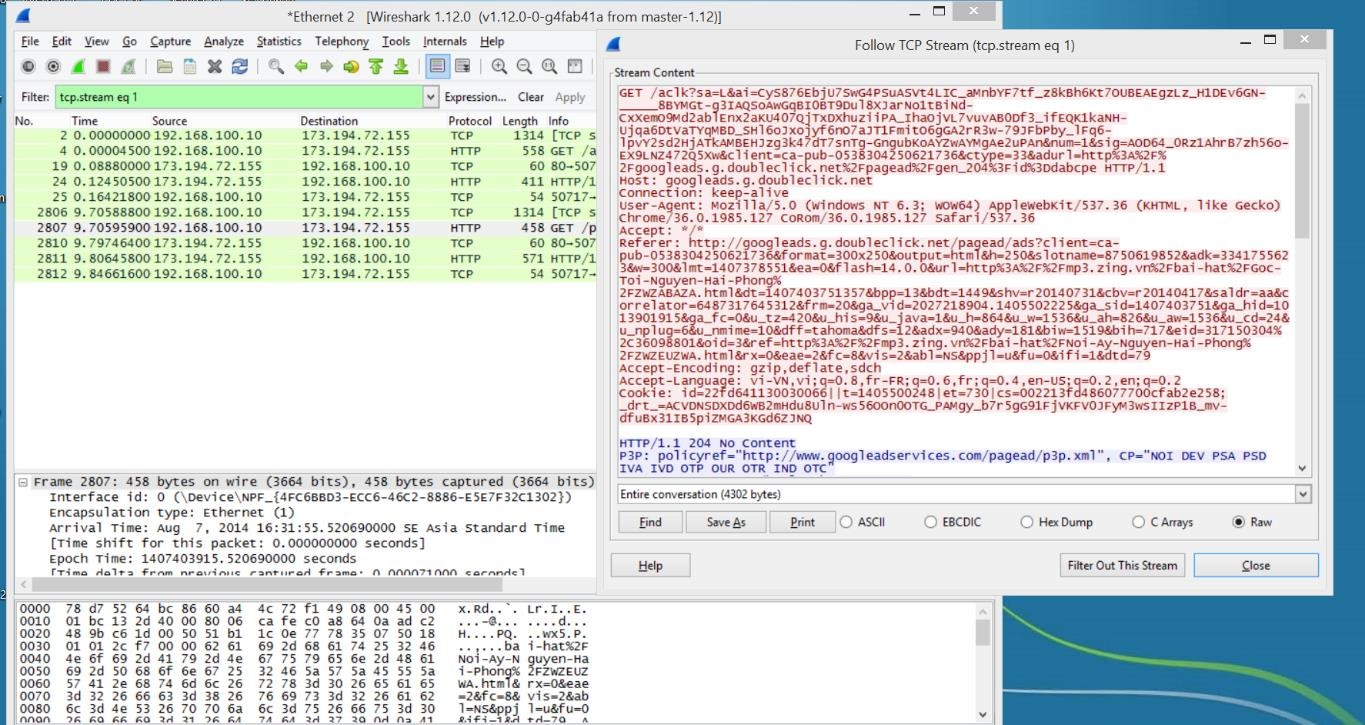
Hoặc nhấn menu Analyze > Display Filters để tạo filter mới:



***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

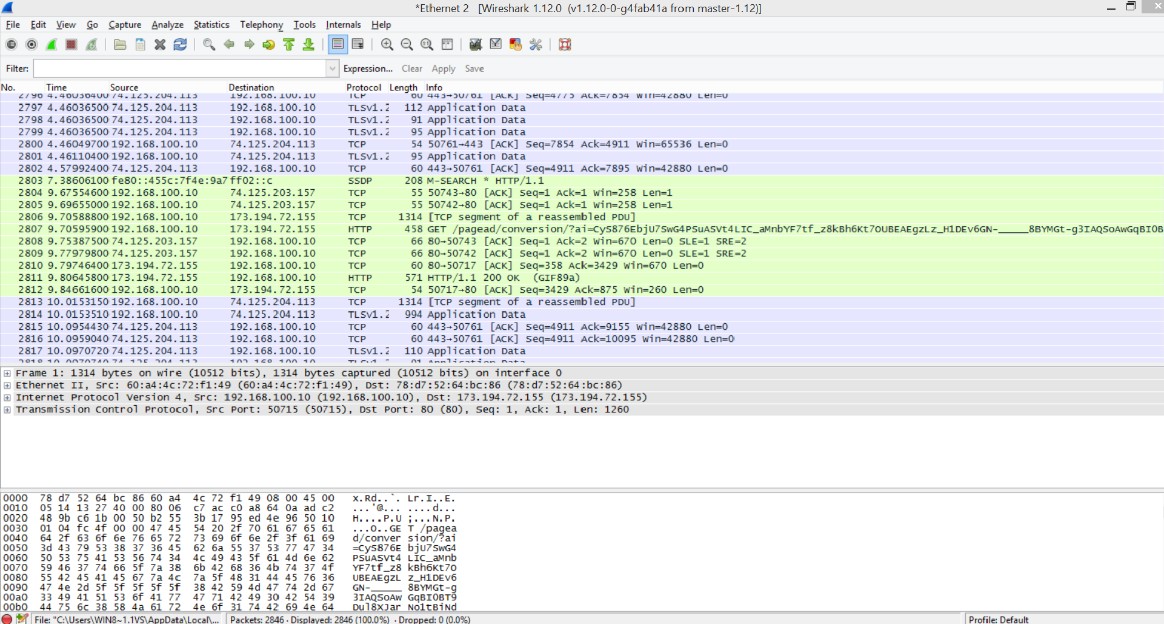
Cài đặt thành công công cụ chặn bắt gói tin wireshark và thư viện winpcap trên môi trường Windows

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

