BÀI THỰC HÀNH SỐ 0

**PHÂN TÍCH LƯU LƯỢNG MẠNG**

**Mục đích:**

Phân tích lưu lượng mạng là một trong những kỹ năng cơ bản và cần thiết đối với người quản trị mạng và an toàn bảo mật hệ thống. Việc phân tích lưu lượng mạng cho phép người quản trị quan sát được trạng thái hoạt động của các giao thức và dịch vụ trong mạng, qua đó có thể đưa ra những nhận định ban đầu về trạng thái an toàn bảo mật của mạng. Bài thực hành này hướng dẫn các thao thác sử dụng cơ bản trên phần mềm Wireshark để phân tích đặc điểm của một số giao thức và dịch vụ phổ biến trong mạng.

**Môi trường thực hành:**

* Hệ điều hành: Microsoft Windows 7, 8, 10
* Các công cụ: Wireshark

**I. Giới thiệu về công cụ Wireshark**

Wireshark là một công cụ kiểm tra, theo dõi và phân tích thông tin mạng được phát triển bởi Gerald Combs. Phiên bản đầu tiên của Wireshark mang tên Ethereal được phát hành năm 1988. Đến nay, WireShark vượt trội về khả năng hỗ trợ các giao thức (khoảng 850 loại), từ những loại phổ biến như TCP, IP đến những loại đặc biệt như là AppleTalk và Bit Torrent. Các tiện ích của phần mềm Wireshark:

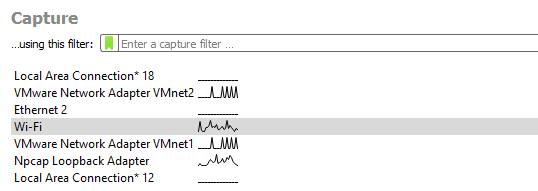
* Thân thiện với người dùng: Giao diện của Wireshark là một trong những giao diện phần mềm phân tích gói dễ dùng nhất. Wireshark là ứng dụng đồ hoạ với hệ thống menu rât rõ ràng và được bố trí dễ hiểu.
* Miễn phí: Wireshark là một sản phẩm miễn phí. Bạn có thể tải về và sử dụng Wireshark cho bất kỳ mục đích nào, kể cả với mục đích thương mại.
* Hỗ trợ: Cộng đồng của Wireshark là một trong những cộng đồng tốt và năng động nhất của các dự án mã nguồn mở.
* Đa nền tảng: Wireshark hỗ trợ hầu hết các loại hệ điều hành hiện nay.

**Các bước sử dụng các tính năng cơ bản của Wireshark như sau:**

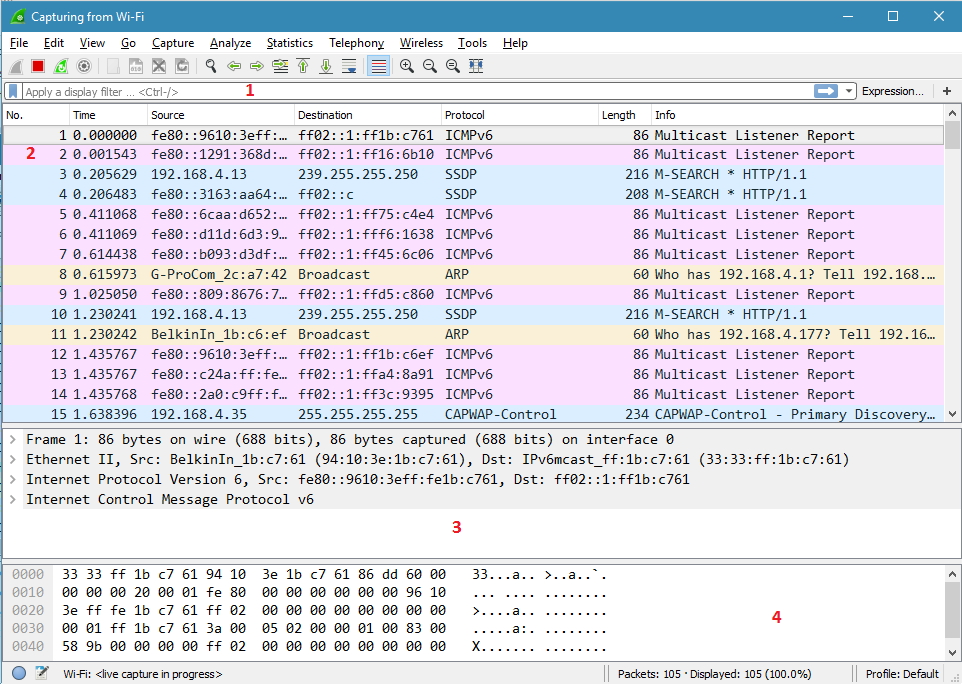
* **Bước 1 :** Download chương trình tại địa chỉ sau và cài đặt như các phần mềm thông thường

**http://www.wireshark.org/download.html**

* **Bước 2 :** Khởi động chương trình. Trên giao diện sau khi khởi động, chú ý đến vùng Capture. Vùng này sẽ liệt kê các cổng mạng có thể bắt và phân tích gói tin.



* **Bước 3**: Trong danh sách được liệt kê, chọn một cổng mạng để bắt đầu quá trình bắt gói tin. Giao diện phân tích các gói tin đã bắt như sau
* Thanh công cụ : Xem mục **Help** của phần mềm để biết thêm chi tiết
* Vùng 1 : Tạo bộ lọc cho phép quan sát các gói tin thỏa mãn yêu cầu nào đó
* Vùng 2 : Danh sách các gói tin đã bắt.
* ***No.*** : Số thứ tự gói tin
* ***Time*** : thời điểm bắt (tính bằng giây kể từ khi bắt đầu)
* ***Source*** : Địa chỉ nguồn của gói tin
* ***Destination*** : Địa chỉ đích của gói tin
* ***Protocol*** : Giao thức. Mỗi gói tin theo giao thức nào đó sẽ có màu được quy ước.
* ***Length*** : Kích thước
* ***Info*** : các thông tin chính về gói tin (thường lấy từ header của gói tin)
* Vùng 3 : Các nội dung phân tích được ở tất cả các tầng trong mô hình TCP/IP.
* Vùng 4 : Nội dung thực tế của gói tin

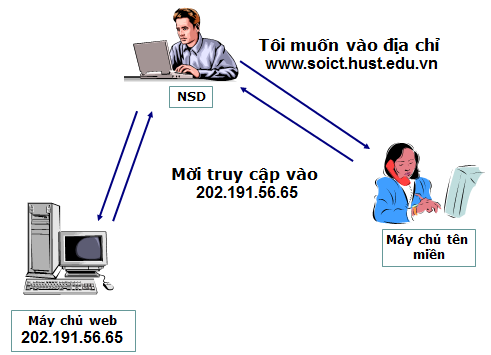
****

* **Bước 3** : Sau một thời gian quan sát, có thể ngừng việc bắt gói tin bằng cách nhấp vào biểu tượng  hoặc phím tắt **Ctrl + E.** Sau đó lưu lại file phân tích dưới dạng **.pcap**
* **Bước 4** : Lựa chọn một gói ở vùng 2 và quan sát nội dung hiển thị ở vùng 3 và 4

**II. Giới thiệu một số giao thức và dịch vụ trong mạng**

1. **Dịch vụ phân giải tên miền DNS**

Tên miền là một chuỗi ký tự định danh cho dịch vụ trên tầng ứng dụng trên một nút mạng nào đó. Người sử dụng có thể dễ dàng truy cập vào dịch vụ thông qua tên miền, thay vì phải nhớ chuỗi các số trong địa chỉ IP. Tuy nhiên, khi máy tính của người sử dụng và máy chủ cung cấp dịch vụ thực hiện trao đổi dữ liệu, chúng sẽ sử đụng địa chỉ IP. Do đó, dịch vụ phân giải tên miền DNS ra đời để thực hiện tìm kiếm địa chỉ IP tương ứng với một tên miền nào đó. Thông thường, khi người sử dụng truy cập vào dịch vụ bằng tên miền, trước hết máy trạm của người dùng sẽ phát yêu cầu sử dụng dịch vụ DNS để phân giải tên miền đó. Hình vẽ dưới đây mô tả trường hợp người sử dụng truy cập vào một Website.



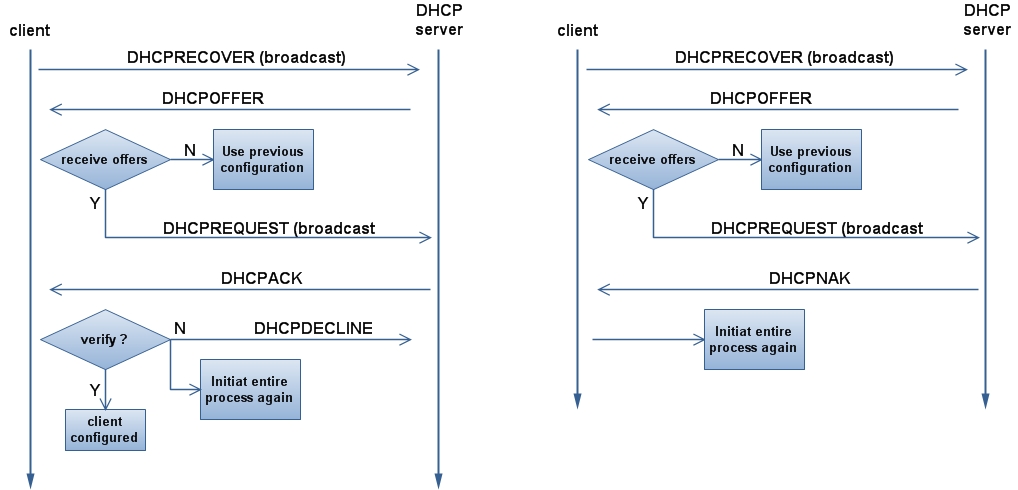
Quá trình phân giải tên miền có thể mô tả ngắn gọn như sau:

* Bước 1: Máy khách gửi thông điệp DNS Query chứa tên miền cần phân giải tới máy chủ DNS
* Bước 2: Máy chủ DNS thực hiện tìm kiếm thông tin tên miền có trong DNS Query
* Bước 3: Máy chủ DNS gửi thông điệp DNS Response chứa kết quả phân giải tên miền

1. **Dịch vụ DHCP(Dynamic Host Configuration)**

DHCP (phiên bản cho IPv6 là DHCPv6) là dịch vụ cấp phát các thông số cấu hình IP cho các máy trạm trong mạng. Các thông số cấp phát bao gồm: địa chỉ IP của máy trạm, mặt nạ mạng, địa chỉ của gateway mặc định, địa chỉ DNS Server, thời hạn sử dụng cấu hình. Các máy trạm tự động cấu hình theo các thông số được cấp phát bởi dịch vụ DHCP. Điều này đem lại lợi ích cho người quản trị mạng trong quá trình triển khai hệ thống mạng. Hoạt động cấp phát thông số cấu hình cho máy trạm có thể mô tả ngắn gọn như sau:

* **Bước 1:** Một máy trạm khi mới kết nối vào trong mạng sẽ gửi thông điệp DHCP Discover theo phương thức quảng bá lên mạng
* **Bước 2**: Nếu có máy chủ DHCP Server trong mạng nhận được thông điệp DHCP Discover, nó sẽ gửi cho máy trạm thông điệp DHCP Offer mang theo các thông số cấu hình
* **Bước 3:** Máy trạm có thể nhận được nhiều thông điệp DHCP Offer khác nhau. Máy trạm chọn một cấu hình từ các thông điệp DHCP Offer khác nhau và gửi thông điệp DHCP Request theo phương thức quảng bá để đăng ký sử dụng.
* **Bước 4:** Máy chủ DHCP Server nhận được thông điệp DHCP Request sẽ kiểm tra thông tin đăng ký. Nếu thông tin này chứa thông số do DHCP Server quản lý, nó gửi thông điệp DHCP ACK để cho phép máy trạm sử dụng. Ngược lại, DHCP Server bỏ qua thông điệp DHCP Request.
* **Bước 5:** Sau khi nhận được thông điệp DHCP ACK, máy trạm bắt đầu sử dụng thông số cấu hình IP đã được cấp phát



Ngoài ra, trong hoạt động, giao thức DHCP còn sử dụng một số gói tin như DHCP Decline, DHCP NACK để xử lý các lỗi phát sinh.

1. **Giao thức ICMP(Internet Control Message Protocol)**

Giao thức ICMP(phiên bản cho IPv6 là ICMPv6) nằm ở tầng mạng, thực hiện chức năng điều khiển trao đổi các thông điệp kiểm tra, truy vấn thông tin trạng thái của các nút mạng. ICMP được coi là giao thức hỗ trợ hoạt động cho giao thức cơ sở của tầng mạng là IP do giao thức IP không thực hiện cơ chế truyền thông tin cậy. Hoạt động của giao thức ICMP rất đơn giản:

* Bước 1: Nút nguồn gửi thông điệp ICMP Request để kiểm tra thông tin trạng thái hoạt động, trạng thái kết nối tới một nút mạng khác
* Bước 2: Nút mạng nhận thông điệp ICMP Request gửi lại thông điệp ICMP Reply để trả lời.

Bên cạnh đó, thông điệp ICMP còn được sử dụng để thông báo lỗi trong quá trình chuyển tiếp gói tin IP trên các nút mạng.

Người quản trị mạng có thể chủ động sử dụng các công cụ dựa trên cơ chế hoạt động của ICMP như ping và traceroute để kiểm tra tình trạng của hệ thống mạng.

* 1. **Lệnh ping**

Lệnh ping cho phép kiểm tra nhanh tình trạng kết nốt và tình trạng hoạt động của một nút mạng. Khi thực hiện lệnh ping, nút nguồn gửi đi thông điệp ICMP Echo Request và đợi thông điệp trả lời.

Cú pháp: **ping Địa\_chỉ\_nút\_đích**

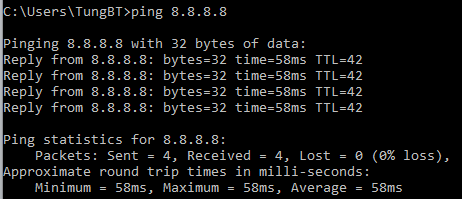
**Địa\_chỉ\_nút\_đích** có thể là một địa chỉ IP hoặc tên miền của máy đích mà ta cần kiểm tra. Hình ảnh sau minh họa kết quả thực hiện lệnh ping tới máy chủ phân giải tên miền của Google:

Lệnh ping cung cấp một số tùy chọn hữu ích khác:

-l Kích\_thước\_thông\_điệp: chỉ định kích thước thông điệp ICMP Echo Request

-n Số\_thông\_điệp\_gửi\_đi

-i Giá trị\_TTL\_của\_thông\_điệp\_gửi\_đi



**3.1. Lệnh tracert**

Lệnh tracert được sử dụng để thu thập thông tin các nút trung gian từ nút nguồn tới nút đích. Khi lệnh tracert được thực hiện, nút nguồn gửi các gói tin có giá trị TTL tăng dần từ 1. Khi thực hiện chuyển tiếp gói tin IP, các nút chuyển tiếp sẽ giảm giá trị TTL đi 1 đơn vị. Nếu giá trị TTL = 0, nút chuyển tiếp gửi thông điệp ICMP báo lỗi cho nút nguồn. Dựa trên việc thu thập các thông điệp báo lỗi này, nút nguồn sẽ có thông tin về các nút trung gian.

Cú pháp: **tracert Địa\_chỉ\_nút\_đích**

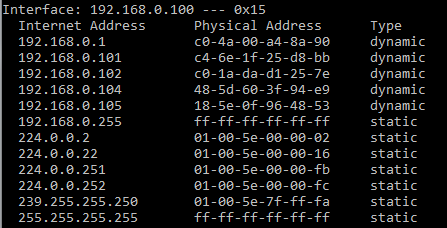
**Địa\_chỉ\_nút\_đích** có thể là một địa chỉ IP hoặc tên miền của máy đích mà ta cần kiểm tra. Hình ảnh sau đây minh họa kết quả thực hiện lệnh tracert để hiển thị thông tin đường đi tới máy chủ phân giải tên miền của Google:



1. **Giao thức ARP (Address Resolution Protocol)**

Giao thức ARP có chức năng tìm kiếm địa chỉ MAC của một nút mạng khi biết địa chỉ IP của nút đó. Trong quá trình truyền dữ liệu, một nút phải xác định địa chỉ MAC của nút kế tiếp để thực hiện đóng gói dữ liệu tại tầng liên kết dữ liệu. Giao thức ARP chỉ hoạt động trong mạng cục bộ. Quá trình hoạt động của giao thức ARP có thể mô tả đơn giản như sau:

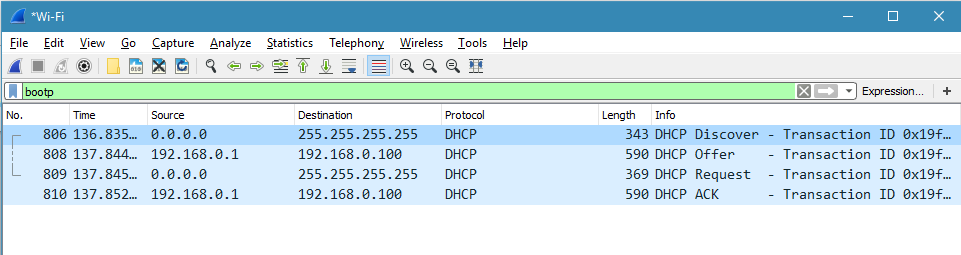
* Bước 1: Nút mạng A nào đó gửi gói tin ARP Request theo phương thức quảng bá lên mạng để tìm kiếm địa chỉ MAC của một nút B. Gói tin ARP Request mang theo địa chỉ IP của nút mạng đang cần tìm kiếm.
* Bước 2: Khi nhận được gói tin ARP Request, nút mạng kiểm tra địa chỉ IP trong gói tin có phải là địa chỉ của nó hay không. Nếu đúng, nó gửi gói tin ARP Response chứa địa chỉ MAC của mình cho A
* Bước 3: A nhận được gói tin ARP Response, ghi lại thông tin địa chỉ MAC tìm kiếm được vào bảng ARP Table. Để xem bảng ARP Table trên hệ điều hành Windows, ta có thể sử dụng lệnh **arp –a**



**III. Nội dung thực hành**

1. **Phân tích lưu lượng dịch vụ DHCP**

* Bước 1: Nhấn tổ hợp phím Windows + R. Gõ lệnh **cmd** để khởi động cửa sổ Command Prompt
* Bước 2: Gõ lệnh **ipconfig /release** trên cửa sổ Command Prompt để giải phóng các thông số cấu hình đang sử dụng
* Bước 3: Khởi động phần mềm Wireshark và chọn cạc mạng phù hợp để bắt gói tin
* Bước 4: Gõ lệnh **ipconfig /renew** trên cửa sổ Command Prompt để xin cấp phát cấu hình mới
* Bước 5: Sau khi lệnh **ipconfig /renew** thực hiện xong, dừng bắt gói tin trên Wireshake và lưu kết quả bắt gói tin với tên **dhcp.pcap**
* Bước 6: Gõ tên giao thức **bootp** vào bộ lọc gói tin của Wireshark. Kết quả hiển thị trên màn hình Wireshark như sau:

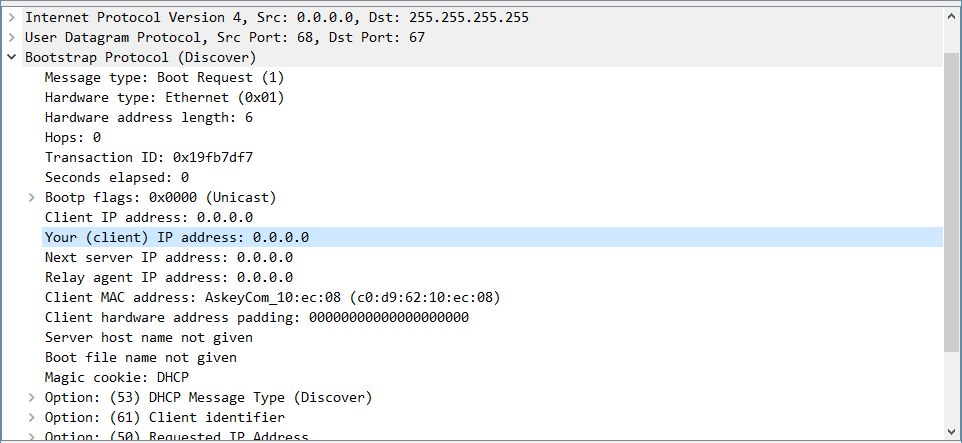


**Phân tích thông tin trên các thông điệp DHCP Discover:**

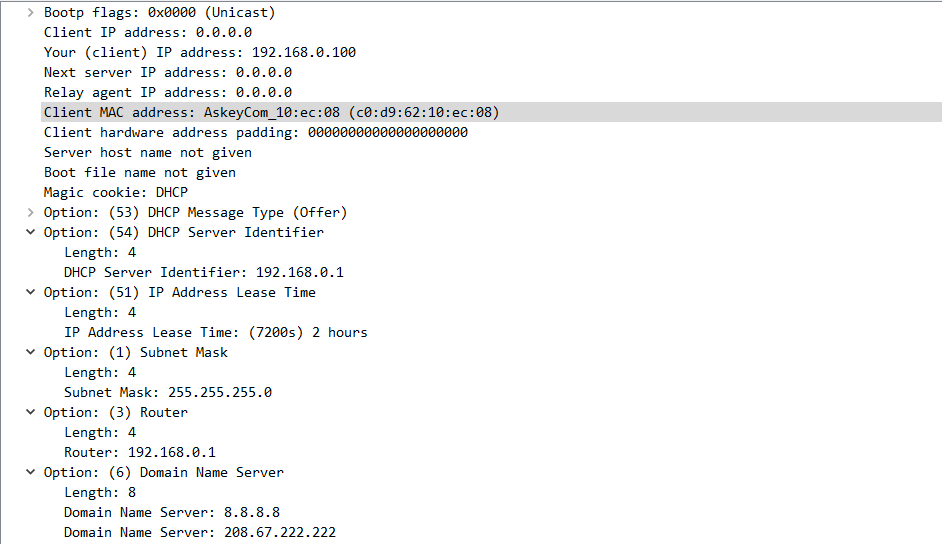
Các thông điệp DHCP được đóng gói tại tầng giao vận theo giao thức UDP

1. Thông điệp DHCP Discover:

* Tiêu đề IP:
* Địa chỉ nguồn(Src): 0.0.0.0 (do máy trạm chưa có địa chỉ IP)
* Địa chỉ đích(Dst): 255.255.255.255 (địa chỉ quảng bá)
* Tiêu đề UDP:
* Số hiệu cổng nguồn(Src Port): 68 (DHCP Client)
* Số hiệu cổng đích(Dst Port): 67 (DHCP Server)
* Thông điệp DHCP Discover:
* Client IP address(Địa chỉ của máy trạm): 0.0.0.0
* Your (client) IP address (Địa chỉ cấp phát cho máy trạm): 0.0.0.0
* Client MAC address (Địa chỉ MAC của máy trạm): c0:d9:62:10:ec:08
* DHCP message Type: Discover

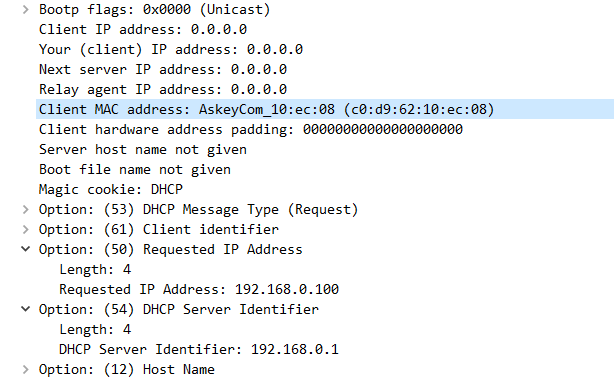


1. Thông điệp DHCP Offer:



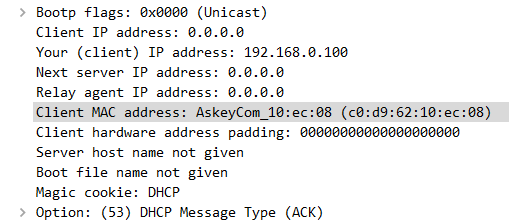
* Client IP address(Địa chỉ của máy trạm): 0.0.0.0
* Your (client) IP address (Địa chỉ cấp phát cho máy trạm): 192.168.0.100
* Client MAC address (Địa chỉ MAC của máy trạm): c0:d9:62:10:ec:08
* DHCP Server Identifier(Địa chỉ DHCP Server): 192.168.0.1
* IP Address Lease Time(Thời gian sử dụng cấu hình): 2 giờ
* Subnet Mask (Mặt nạ mạng): 255.255.255.0
* Router (Địa chỉ gateway mặc định): 192.068.0.1
* Domain Name Server(Địa chỉ máy chủ DNS): 8.8.8.8 và 208.67.222.222
* DHCP message Type: Offer

1. Thông điệp DHCP Request



* Client IP address(Địa chỉ của máy trạm): 0.0.0.0
* Your (client) IP address (Địa chỉ cấp phát cho máy trạm): 0.0.0.0
* Client MAC address (Địa chỉ MAC của máy trạm): c0:d9:62:10:ec:08
* Requested IP Address (Địa chỉ IP yêu cầu được sử dụng): 192.168.0.100
* DHCP message Type: Request

1. Thông điệp DHCP ACK

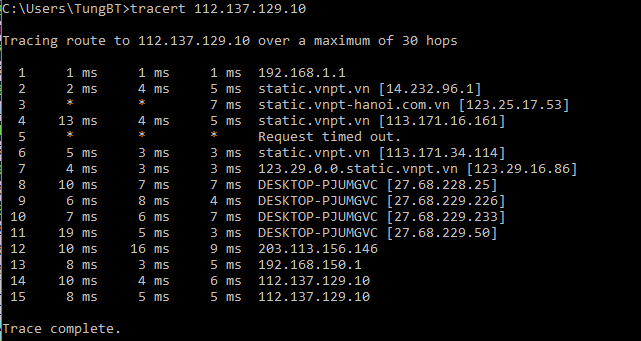


* Client IP address(Địa chỉ của máy trạm): 0.0.0.0
* Your (client) IP address (Địa chỉ cấp phát cho máy trạm): 192.168.0.100
* Client MAC address (Địa chỉ MAC của máy trạm): c0:d9:62:10:ec:08
* DHCP message Type: ACK

1. **Phân tích lưu lượng ICMP**

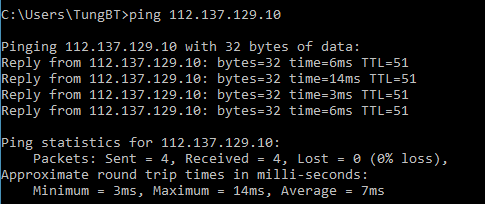
* **Bước 1:** Khởi động chương trình Wireshark để bắt gói tin trên cạc mạng phù hợp
* **Bước 2:** Thực hiện lệnh **tracert 112.137.129.10**

Chờ lệnh thực hiện xong trước khi chuyển sang bước tiếp theo.



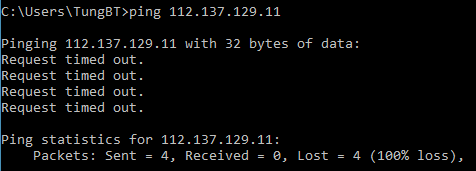
* **Bước 3:** Thực hiện lệnh **ping 112.137.129.10**

Chờ lệnh thực hiện xong trước khi chuyển sang bước tiếp theo.



* **Bước 4:** Thực hiện lệnh **ping 112.137.129.11**

Chờ lệnh thực hiện xong trước khi chuyển sang bước tiếp theo.



* **Bước 5**: Khi lệnh thực hiện xong, quay trở lại cửa sổ chương trình Wireshark, dừng việc bắt gói tin và lưu lại file với tên **ip.pcap**
* **Bước 6:** Điền giá trị sau vào bộ lọc để lọc các gói tin:

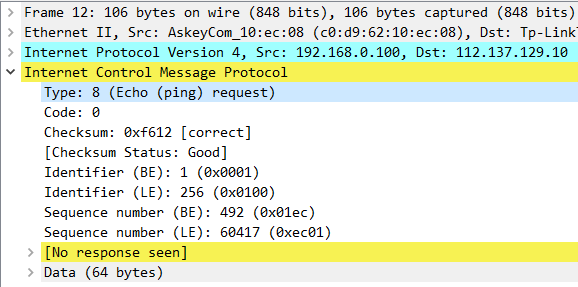
**icmp && ip.addr == 112.137.129.10**

**Phân tích lưu lượng ICMP**

****

Quan sát kết quả bắt gói tin có thể thấy:

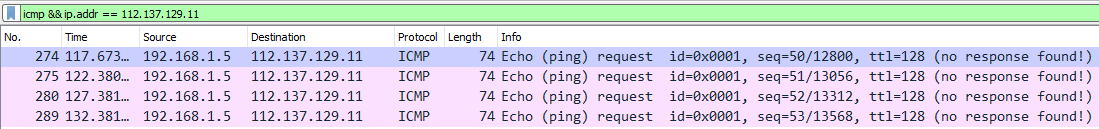
* Các gói tin ICMP do nút nguồn (địa chỉ 192.168.0.100) gửi đi có giá trị TTL tăng dần. Các gói tin này có Type = 8 (ICMP Echo Request) và kích thước mặc định 64 bytes



* Địa chỉ nguồn của các gói tin ICMP báo lỗi Time-to-live exceeded (Type = 11) chính là địa chỉ mà lệnh tracert thu nhận được
* Đối với lưu lượng khi thực hiện lệnh ping, với mỗi gói tin ICMP Echo Request gửi đi, nút nguồn nhận được một gói tin ICMP Echo Reply. Điều này phù hợp với kết quả thực hiện lệnh ping tới địa chỉ 112.137.129.10 cho thấy kết nối tới nút mạng này là bình thường
* **Bước 7:** Điền giá trị sau vào bộ lọc để lọc các gói tin:

**icmp && ip.addr == 112.137.129.11**

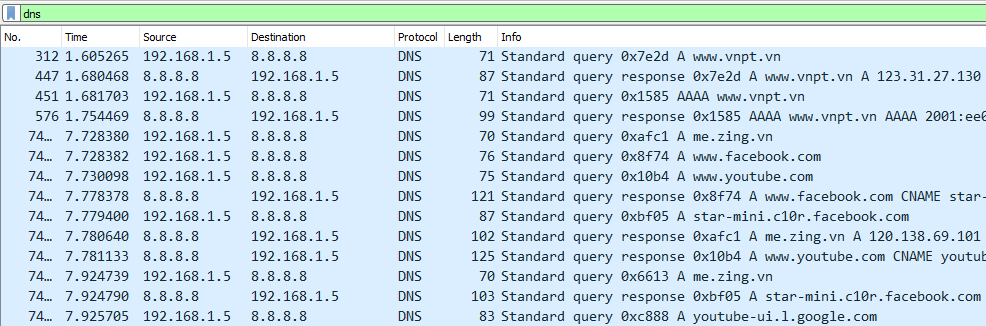
Phân tích lưu lượng ICMP khi thực hiện lệnh ping tới địa chỉ 112.137.129.11

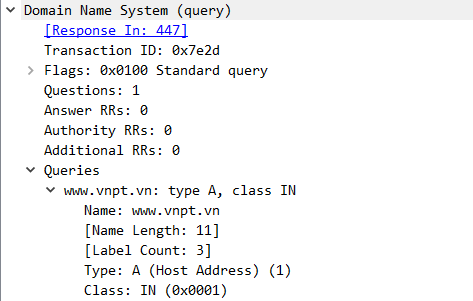


Kết quả cho thấy không có gói tin ICMP Echo Reply trả lời. Điều này phù hợp với kết quả thực hiện lệnh ping tới địa chỉ 112.137.129.11 cho thấy không thể kết nối tới nút mạng này.

1. **Phân tích lưu lượng DNS**

* **Bước 1:** Tắt các chương trình của người dùng có trao đổi dữ liệu trên mạng trừ trình duyệt Web. Trên trình duyệt Web chỉ để lại một tab trắng, chưa truy cập vào bất kỳ website nào.
* Mozilla Firefox: Nhấn tổ hợp phím **Ctrl + Shift + Del**. Chọn **Today.** Chọn **Cache**. Nhấp nút **Clear Now**
* Google Chrome: Nhấn tổ hợp phím **Ctrl + Shift + Del**. Chọn **the past day**. Chọn **Cached images and files**. Nhấp nút **Clear browsing data**.
* **Bước 2:** Trên cửa sổ Command Prompt, thực hiện lệnh **ipconfig /flushdns**
* **Bước 2:** Khởi động phần mềm Wireshark và chọn bắt gói tin trên cạc mạng phù hợp
* **Bước 3:** Truy cập vào website vnpt.vn. Sau khi trang web được tải xong, dừng bắt gói tin và lưu kết quả với tên file là web.pcap
* **Bước 4:** Điền giá trị **dns** vào bộ lọc để lọc các gói tin.

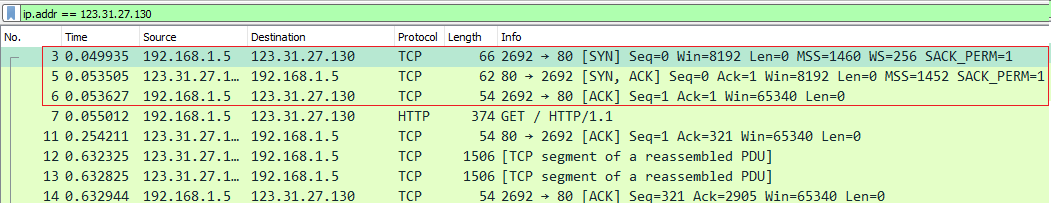


**Phân tích lưu lượng DNS:**

* Chọn thông điệp DNS Standard query, giả sử có số thứ tự 312. Phân tích phần Queries trong thông điệp cho thấy thông tin sau:
* Name(tên miền cần truy vấn): vnpt.vn
* Type(Loại thông tin tên miền cần truy vấn): A(truy vấn địa chỉ IPv4)
* Với truy vấn địa chỉ IPv6, Type có giá trị là AAAA
* Chọn thông điệp DNS Standard Query Response trả lời cho truy vấn trên. Trong ví dụ này thông điệp đó được đánh số 447 do mang giá trị Transaction ID là 0x7e2d trùng với giá trị tương ứng của thông điệp truy vấn. Phân tích gói tin cho thấy thông tin sau:
* Phần Queries mang thông tin tương tự thông điệp truy vấn
* Phần Answers mang theo kết quả truy vấn trong trường Address là địa chỉ 123.31.27.130 là địa chỉ IP của máy chủ Web vnpt.vn
* Ngoài các thông điệp DNS thực hiện truy vấn tên miền vnpt, chúng ta có thể quan sát thấy rất nhiều thông điệp thực hiện các truy vấn khác. Nguyên nhân là trong mã nguồn HTML của website vnpt.vn có các đối tượng Web, đường dẫn nằm trên các web server khác. Có thể kiểm chứng sự xuất hiện của các tên miền này khi xem mã nguồn HTML của trang web.

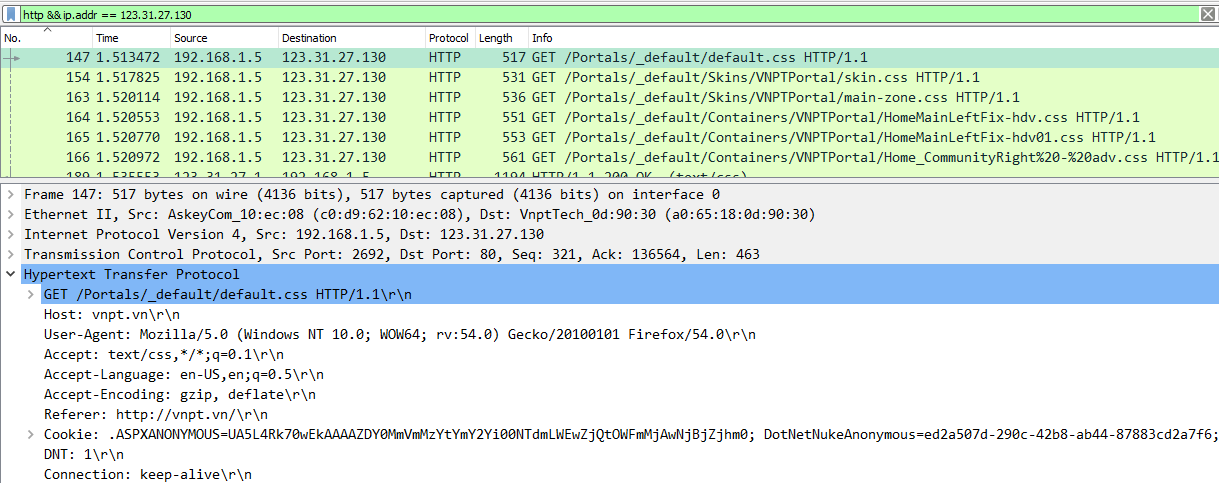
1. **Phân tích lưu lượng khi truy cập dịch vụ Web**

* Sử dụng file bắt lưu lượng web.pcap ở phần 3 với giá trị bộ lọc là **ip.addr == 123.31.27.130**



Có thể thấy, trình duyệt Web và máy chủ Web đã thiết lập kết nối TCP trước khi trao đổi các thông điệp HTTP

* Thay đổi giá trị bộ lọc là **http && ip.addr == 123.31.27.130**. Chọn một thông điệp HTTP Request nào đó, ví dụ thông điệp 147



Phân tích tiêu đề của thông điệp này, chúng ta có thể thu được một số thông tin sau:

* Phương thức yêu cầu: GET
* Đối tượng yêu cầu: /Portals/\_default/default.css
* Host(Máy chủ Web): vnpt.vn
* User-Agent(Web client): Mozilla Firefox 54.0, chạy trên hệ điềuhành Windows 10.0 64-bit
* Referer(Địa chỉ của trang web phát sinh thông điệp yêu cầu): vnpt.vn
* Cookie: Dựa trên nội dung cookie có thể thấy website vnpt.vn xây dựng trên nền tảng .NetNuke

Chọn thông điệp HTTP Response trả lời là gói tin số 189. Phân tích tiêu đề của thông điệp này, chúng ta có thể thu được một số thông tin sau:

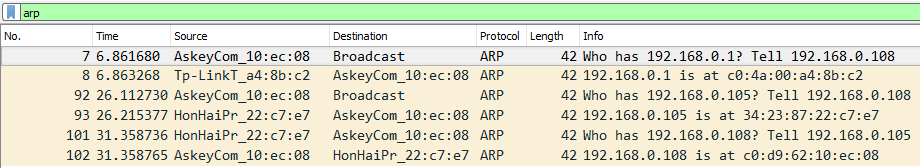
* Mã trả lời: 200 (yêu cầu đã được đáp ứng thành công)
* Last-Modified (Thời điểm cuối cùng đối tượng Web được cập nhật): Wed, 20 Mar 2013 10:17:34 GMT
* Server(Thông tin máy chủ Web): sử dụng phần mềm Web Server Microsoft-IIS/7.0
* Thời điểm đáp ứng: Mon, 24 Jul 2017 14:20:47 GMT

Phần thân thông điệp chứa dữ liệu trả lời có thể xem chi tiết ở trường Line-based text data.

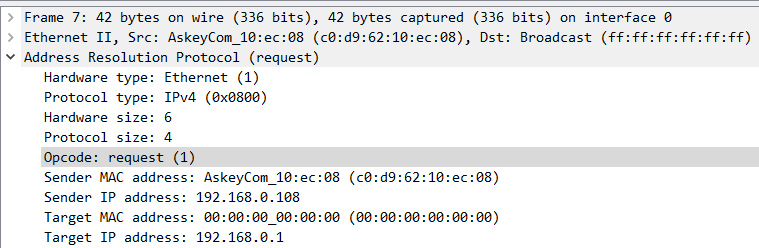
1. **Phân tích lưu lượng ARP**

* **Bước 1:** Khởi động phần mềm Wireshark và chọn bắt gói tin trên cạc mạng phù hợp
* **Bước 2:** Mở cửa sổ Command Prompt với quyền Administrator và thực hiện lệnh **arp –d \***
* **Bước 3:** Điền giá trị **arp** vào bộ lọc và đợi phần mềm bắt được một số gói tin thì dừng lại.

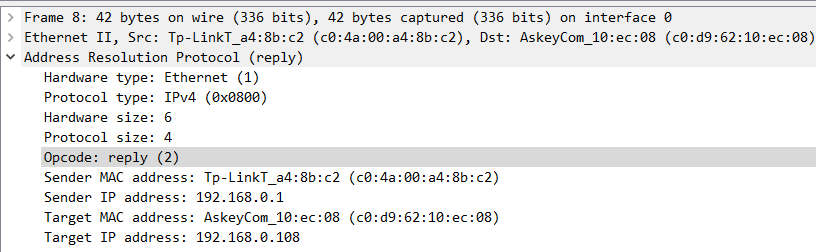
**Phân tích lưu lượng ARP:**



* Chọn gói tin gửi theo phương thức broadcast, giả sử trong ví dụ này là gói số 7.



* Opcode: 1(Thông điệp yêu cầu)
* Target IP address(địa chỉ IP của nút cần tìm địa chỉ MAC): 192.168.0.1
* Target MAC address(Địa chỉ MAC của nút cần tìm):00:00:00:00:00:00(chưa xác định)
* Chọn gói tin số 8 là gói tin ARP Reply chứa kết quả trả lời:



* Opcode: 2(Thông điệp trả lời)
* Sender IP address(Địa chỉ IP của nút gửi trả lời): 192.168.0.1
* Sender MAC address (Địa chỉ MAC của nút trả lời): c0:4a:00:a4:8b:c2

**III. Luyện tập**

1. **Phân tích lưu lượng ICMP**

Thực hiện các bước tương tự mục II.2 với các địa chỉ IP lần lượt là 210.86.226.162 và 210.86.226.163

1. **Phân tích lưu lượng DNS và Web**

Thực hiện các bước tương tự mục II.3 và II.4 với địa chỉ Website cần truy cập là [http://mso.soict.hust.edu.vn/~tungbt/it3080/lab01](http://nct.soict.hust.edu.vn/~tungbt/it3080/lab01)

**Phân tích lưu lượng DNS:**

* Thông điệp DNS query được gửi đến nút mạng địa chỉ IP là gì? Sử dụng lệnh **nm-tool|grep DNS** để xem thông tin địa chỉ DNS server được cấu hình là gì? Hai địa chỉ này giống hay khác nhau.
* Trên thông điệp DNS query để truy vấn thông tin tên miền **soict.hust.edu.vn**, trong mục Queries, kiểu (type) truy vấn là gì?
* Trên thông điệp DNS trả lời, trong mục Queries, kiểu (type) truy vấn là gì?
* Các tên miền được yêu cầu phân giải là gì? Kết quả phân giải ứng với mỗi tên miền

**Phân tích lưu lượng Web:**

* Có bao nhiêu thông điệp HTTP Request đươc phát đi? Mỗi thông điệp này được sử dụng để yêu cầu đối tượng nào?

|  |  |  |  |
| --- | --- | --- | --- |
| STT gói tin | Phương thức HTTP | Đối tượng yêu cầu | Mã trả lời trên thông điệp HTTP Response tương ứng |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

* Thông tin về trình duyệt Web và hệ điều hành trên máy trạm người dùng
* Thông tin về phần mềm Web server và hệ điều hành trên máy chủ