

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH TN (CO3094)

BÀI TẬP LAB 2B

WIRESHARK DNS

LỚP: L09

GVHD: Bùi Xuân Giang

Sinh viên thực hiện

Nguyễn Tấn Tài : 2212990

Thành phố Hồ Chí Minh, tháng 9 năm 2024

Như được mô tả trong Mục 2.4 của sách giáo khoa, Hệ thống Tên Miền (DNS) chuyển đổi tên miền thành địa chỉ IP, đóng một vai trò quan trọng trong cơ sở hạ tầng Internet. Trong bài thực hành này, chúng ta sẽ tìm hiểu kỹ hơn về phía máy khách của DNS. Hãy nhớ rằng vai trò của máy khách trong DNS khá đơn giản – máy khách gửi một truy vấn tới máy chủ DNS cục bộ của nó và nhận về một phản hồi. Như được minh họa trong Hình 2.19 và 2.20 trong sách giáo khoa, nhiều thứ có thể diễn ra "dưới bề mặt", vô hình với các máy khách DNS, vì các máy chủ DNS phân cấp sẽ giao tiếp với nhau để giải quyết truy vấn của máy khách bằng cách sử dụng phương thức đệ quy hoặc lặp. Từ góc nhìn của máy khách DNS, tuy nhiên, giao thức này khá đơn giản – một truy vấn được định dạng gửi đến máy chủ DNS cục bộ và một phản hồi được nhận lại từ máy chủ đó.

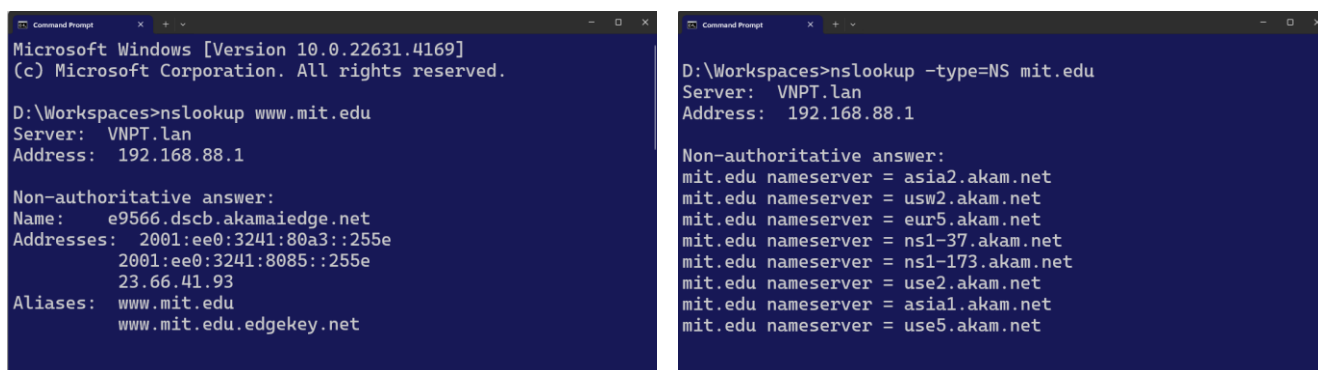
Trước khi bắt đầu bài thực hành này, bạn có thể muốn xem lại DNS bằng cách đọc Mục 2.4 của sách giáo khoa. Đặc biệt, bạn có thể muốn xem lại phần tài liệu về máy chủ DNS cục bộ, lưu trữ DNS (DNS caching), bản ghi và thông điệp DNS, và trường TYPE trong bản ghi DNS.

1. nslookup

Trong bài thực hành này, chúng ta sẽ sử dụng rộng rãi công cụ nslookup, công cụ này có sẵn trên hầu hết các nền tảng Linux/Unix và Microsoft hiện nay. Để chạy nslookup trên Linux/Unix, bạn chỉ cần nhập lệnh nslookup trên dòng lệnh. Để chạy nó trên Windows, mở Command Prompt và chạy nslookup trên command line.

Trong cách sử dụng cơ bản nhất, công cụ nslookup cho phép máy chủ chạy công cụ này truy vấn bất kỳ máy chủ DNS nào được chỉ định để có bản ghi DNS. Máy chủ DNS được truy vấn có thể là máy chủ DNS gốc, máy chủ DNS cấp cao nhất, máy chủ DNS ủy quyền, hoặc máy chủ DNS trung gian (xem sách giáo khoa để biết các định nghĩa về các thuật ngữ này). Để hoàn thành nhiệm vụ này, nslookup gửi một truy vấn DNS đến máy chủ DNS được chỉ định, nhận về một phản hồi DNS từ cùng một máy chủ, và hiển thị kết quả.

Ảnh chụp màn hình dưới đây hiển thị kết quả của lệnh nslookup `www.mit.edu` (được hiển thị trong Command Prompt của Windows). Trong ví dụ này, máy chủ khách đang sử dụng mạng gia đình, nơi máy chủ DNS cục bộ mặc định là VNPT.lan với địa chỉ IP là 192.168.88.1. Khi chạy nslookup, nếu không có máy chủ DNS nào được chỉ định, thì nslookup sẽ gửi truy vấn tới máy chủ DNS mặc định, trong trường hợp này là VNPT.lan.



```

Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

D:\Workspaces>nslookup www.mit.edu
Server: VNPT.lan
Address: 192.168.88.1

Non-authoritative answer:
Name: e9566.dscb.akamaiedge.net
Addresses: 2001:ee0:3241:80a3::255e
           2001:ee0:3241:8085::255e
           23.66.41.93
Aliases: www.mit.edu
          www.mit.edu.edgekey.net

D:\Workspaces>nslookup -type=NS mit.edu
Server: VNPT.lan
Address: 192.168.88.1

Non-authoritative answer:
mit.edu nameserver = asia2.akam.net
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = use5.akam.net

```

Lệnh này có nghĩa là "vui lòng gửi cho tôi địa chỉ IP của máy chủ www.mit.edu". Như được hiển thị trong ảnh chụp màn hình, phản hồi từ lệnh này cung cấp hai mẫu thông tin: (1) tên và địa chỉ IP của máy chủ DNS cung cấp câu trả lời (VNPT.lan, địa chỉ IP 192.168.88.1), và (2) chính câu trả lời, bao gồm tên máy chủ và địa chỉ IP của www.mit.edu. Kết quả này chỉ ra rằng e9566.dscb.akamaiedge.net (một phần của mạng phân phối nội dung Akamai) là máy chủ chịu trách nhiệm phân giải tên miền cho www.mit.edu, với các địa chỉ IP là 23.66.41.93 và hai địa chỉ IPv6.

Mặc dù phản hồi này đến từ máy chủ DNS cục bộ của VNPT, rất có thể máy chủ DNS này đã sử dụng các bản ghi được lưu trong bộ nhớ đệm hoặc liên lạc với các máy chủ DNS khác để nhận câu trả lời.

Bây giờ hãy xem xét lệnh thứ hai:

```
nslookup -type=NS mit.edu
```

Trong ví dụ này, chúng ta đã cung cấp tùy chọn "-type=NS" và miền "mit.edu". Điều này khiến nslookup gửi một truy vấn cho bản ghi type-NS đến máy chủ DNS mặc định (VNPT.lan với địa chỉ IP 192.168.88.1). Về mặt ngôn ngữ, truy vấn này có nghĩa là, "vui lòng gửi cho tôi tên của các máy chủ DNS ủy quyền cho mit.edu."

(Khi không sử dụng tùy chọn **-type**, nslookup sử dụng mặc định, đó là truy vấn cho bản ghi kiểu A). Kết quả trả về chỉ ra rằng MIT đang sử dụng nhiều máy chủ DNS được cung cấp bởi Akamai. Câu trả lời bao gồm các máy chủ tên miền (nameservers) như asia2.akam.net, usw2.akam.net, eur5.akam.net, và các máy chủ khác, trải khắp các khu vực địa lý như châu Á, châu Âu, và Hoa Kỳ. Tuy nhiên, nslookup cũng chỉ ra rằng đây là câu trả lời "non-authoritative"

(không chính thức), có nghĩa là câu trả lời này có thể đến từ bộ nhớ đệm của một số máy chủ khác thay vì từ máy chủ DNS ủy quyền trực tiếp tại MIT. Điều này thường xảy ra khi kết quả được lấy từ một máy chủ DNS trung gian, chẳng hạn như máy chủ DNS của VNPT. Mặc dù truy vấn type-NS không yêu cầu địa chỉ IP, máy chủ DNS đã trả về những tên miền của các máy chủ DNS ủy quyền cho MIT.

Bây giờ hãy xem xét lệnh thứ ba:

```
nslookup www.aiit.or.kr asia1.akam.net
```

Trong ví dụ này, chúng ta chỉ định rằng truy vấn cần được gửi tới máy chủ DNS asia1.akam.net thay vì sử dụng máy chủ DNS mặc định (ví dụ, dns-prime.poly.edu hoặc máy chủ DNS của nhà cung cấp dịch vụ internet). Truy vấn và phản hồi được thực hiện trực tiếp giữa máy khách của bạn và asia1.akam.net, bỏ qua máy chủ DNS mặc định.

```
D:\Workspaces>nslookup www.aiit.or.kr asia1.akam.net
Server: UnKnown
Address: 95.100.175.64

*** UnKnown can't find www.aiit.or.kr: Query refused
D:\Workspaces>
```

```
D:\Workspaces>nslookup www.aiit.or.kr 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: www.aiit.or.kr
Address: 58.229.6.225
```

Tuy nhiên, trong các tình huống thực tế như khi bạn đang sử dụng asia2.akam.net, máy chủ DNS có thể từ chối truy vấn cho các tên miền không thuộc hệ thống mà nó quản lý (trong trường hợp này là mit.edu). Điều này có thể do các chính sách bảo mật hoặc giới hạn truy vấn của máy chủ DNS. Mặc dù asia2.akam.net là một máy chủ DNS ủy quyền cho mit.edu, nó chỉ phục vụ các truy vấn liên quan đến mit.edu và từ chối các truy vấn đến các tên miền bên ngoài, như www.aiit.or.kr. Để tránh tình trạng này, bạn có thể sử dụng máy chủ DNS công cộng như 8.8.8.8 (máy chủ DNS của Google), có khả năng phân giải tên miền toàn cầu.

Ví dụ, bạn có thể thử lệnh sau để phân giải tên miền www.aiit.or.kr:

```
nslookup www.aiit.or.kr 8.8.8.8
```

Trong lệnh này, bạn yêu cầu máy chủ DNS công cộng của Google phân giải tên miền www.aiit.or.kr thay vì sử dụng máy chủ DNS nội bộ hoặc một máy chủ DNS có giới hạn.

Bây giờ, sau khi đã thông qua ba ví dụ minh họa, có thể bạn đang thắc mắc về cú pháp chung của các lệnh **nslookup**. Cú pháp là:

```
nslookup -option1 -option2 host-to-find dns-server
```

Nói chung, nslookup có thể được chạy với 0, 1, 2 hoặc nhiều tùy chọn hơn. Và như chúng ta đã thấy trong các ví dụ trên, dns-server là tùy chọn; nếu không được chỉ định, truy vấn sẽ được gửi tới máy chủ DNS mặc định.

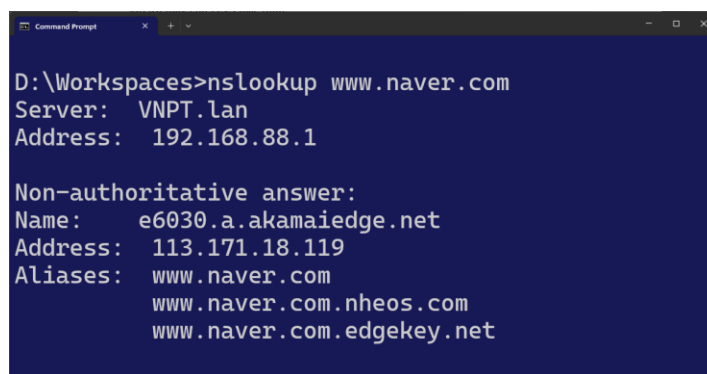
Bây giờ chúng ta đã có cái nhìn tổng quan về **nslookup**, đã đến lúc bạn tự mình trải nghiệm. Hãy làm như sau (và ghi lại kết quả)

Trả lời câu hỏi

1. Chạy nslookup để lấy địa chỉ IP của một máy chủ web ở Châu Á. Địa chỉ IP của máy chủ đó là gì?

Em chọn Naver, là một nền tảng trực tuyến của Hàn Quốc được điều hành bởi Naver Corporation¹². Trang web này là cổng thông tin điện tử lớn tại Hàn Quốc và chiếm lĩnh hơn 70% lượng truy cập tìm kiếm trên internet tại đất nước này.

```
nslookup www.naver.com
```



```
D:\Workspaces>nslookup www.naver.com
Server: VNPT.lan
Address: 192.168.88.1

Non-authoritative answer:
Name: e6030.a.akamaiedge.net
Address: 113.171.18.119
Aliases: www.naver.com
         www.naver.com.nheos.com
         www.naver.com.edgekey.net
```

e6030.a.akamaiedge.net là tên miền thực tế mà máy chủ DNS của bạn đã phân giải cho yêu cầu truy vấn tên miền www.naver.com. Tên miền này thuộc về Akamai, một mạng lưới phân phối nội dung (CDN) toàn cầu. Điều này cho thấy Naver đang sử dụng Akamai để phân phối nội dung của mình, giúp cải thiện tốc độ truy cập và tối ưu hóa tải.

Địa chỉ IP: **113.171.18.119**. Địa chỉ IP này thuộc dải địa chỉ của châu Á (cụ thể là Việt Nam), điều này cho thấy máy chủ Akamai có thể đang phân phối nội dung từ một máy chủ đặt ở gần để tối ưu hóa tốc độ truy cập.

Aliases (Bí danh) chỉ ra rằng www.naver.com có nhiều tên miền liên quan hoặc bí danh để phục vụ cho việc phân phối nội dung.

2. Chạy nslookup để xác định các máy chủ DNS ủy quyền cho một trường đại học ở Châu Âu.

Em chọn Trường Đại học ETH Zurich, chuyên về kỹ thuật và khoa học tự nhiên, được thành lập vào năm 1855 tại thành phố Zürich, Thụy Sĩ. Họ có trang web với tên miền **ethz.ch**.

```
Command Prompt
D:\Workspaces>nslookup -type=NS ethz.ch
Server: VNPT.lan
Address: 192.168.88.1

Non-authoritative answer:
ethz.ch nameserver = ns2.switch.ch
ethz.ch nameserver = ns1.ethz.ch
ethz.ch nameserver = ns2.ethz.ch

ns1.ethz.ch      internet address = 129.132.98.8
ns2.ethz.ch      internet address = 129.132.250.8
ns1.ethz.ch      AAAA IPv6 address = 2001:67c:10ec::a
ns2.ethz.ch      AAAA IPv6 address = 2001:67c:10ec::b
```

Kết quả liệt kê các máy chủ DNS ủy quyền cho miền ethz.ch (Đại học ETH Zurich ở Thụy Sĩ). Đây là các máy chủ có quyền trả lời chính thức cho các truy vấn liên quan đến tên miền ethz.ch, điều này có nghĩa là các máy chủ DNS này chịu trách nhiệm cung cấp thông tin về tên miền ethz.ch.

- ns1.ethz.ch có địa chỉ IP IPv4: 129.132.98.8; IPv6: 2001:67c:10ec::a
- ns2.ethz.ch có địa chỉ IP: IPv4: 129.132.250.8; IPv6: 2001:67c:10ec::b

Máy chủ ns2.switch.ch¹ cũng là một trong những máy chủ DNS ủy quyền cho ethz.ch. switch.ch là tên miền của một tổ chức hạ tầng mạng quan trọng ở Thụy Sĩ, được sử dụng bởi các trường đại học và tổ chức học thuật khác nhau.

¹ [https://portal.switch.ch/pub/public-dns/#:~:text=Public%20DNS%20resolver%20\(beta\)%20for%20the](https://portal.switch.ch/pub/public-dns/#:~:text=Public%20DNS%20resolver%20(beta)%20for%20the)

3. Chạy nslookup để xác minh rằng một trong những máy chủ DNS thu được ở Câu hỏi 2 được truy vấn cho các máy chủ thư Yahoo! chính. Địa chỉ IP của nó là gì?

Mặc dù đã thử nghiệm đối với nhiều trường đại học ở châu Âu, University of Cambridge (cam.ac.uk), University of Edinburgh (ed.ac.uk), Université de Genève (unige.ch), ..., thì tất cả máy chủ DNS của các trường đại học châu Âu từ chối truy vấn (với lỗi Query refused).

Hiện nay điều này là phổ biến, vì nhiều máy chủ DNS của các tổ chức này được cấu hình chỉ để xử lý các truy vấn cho tên miền nội bộ và từ chối các truy vấn đệ quy (recursive queries) từ bên ngoài.

Giải pháp thay thế: em sử dụng các máy chủ DNS công cộng, như: Google Public DNS: 8.8.8.8; Cloudflare DNS: 1.1.1.1

```

Command Prompt
D:\Workspaces>nslookup -type=MX yahoo.com 2001:67c:10ec::b
Server: UnKnown
Address: 2001:67c:10ec::b

*** UnKnown can't find yahoo.com: No response from server

D:\Workspaces>nslookup -type=MX yahoo.com ns2.switch.ch
Server: ns2.switch.ch
Address: 130.59.31.29

*** ns2.switch.ch can't find yahoo.com: Query refused

D:\Workspaces>nslookup -type=MX yahoo.com 129.132.250.8
Server: ns2.ethz.ch
Address: 129.132.250.8

*** ns2.ethz.ch can't find yahoo.com: Query refused

```

```

Command Prompt
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

D:\Workspaces>nslookup -type=MX yahoo.com 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
yahoo.com      MX preference = 1, mail exchanger = mta6.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta7.am0.yahoodns.net
yahoo.com      MX preference = 1, mail exchanger = mta5.am0.yahoodns.net

```

MX preference (còn gọi là trọng số MX) là một giá trị số để chỉ định độ ưu tiên của các máy chủ thư. Số càng thấp, độ ưu tiên càng cao. Trong trường hợp này, cả ba máy chủ MX (mta5, mta6 và mta7) đều có cùng một giá trị ưu tiên là 1. Điều này có nghĩa là các máy chủ này được xem như có độ ưu tiên ngang nhau, và bất kỳ máy chủ nào cũng có thể được sử dụng để nhận email cho yahoo.com.

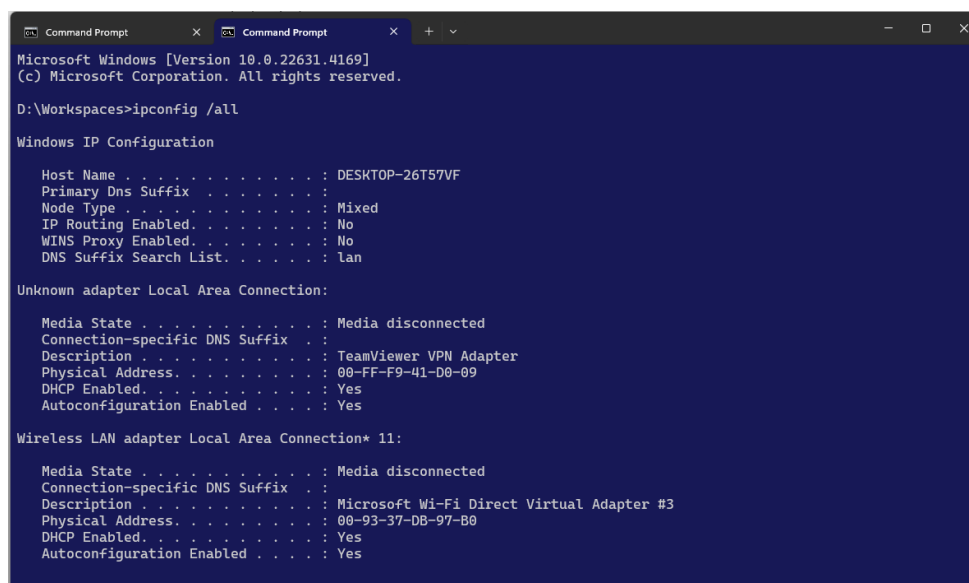
mta5.am0.yahoodns.net, mta6.am0.yahoodns.net, và mta7.am0.yahoodns.net là các máy chủ trao đổi thư (mail exchanger) được cấu hình để nhận email cho yahoo.com. Đây là các máy chủ của Yahoo để xử lý email đến.

2. ipconfig

ipconfig (dành cho Windows) và ifconfig (dành cho Linux/Unix) là hai tiện ích rất hữu dụng trong máy chủ của bạn, đặc biệt trong việc khắc phục sự cố mạng. Ở đây, chúng ta chỉ mô tả ipconfig, mặc dù ifconfig trên Linux/Unix cũng rất giống. ipconfig có thể được sử dụng để hiển thị thông tin TCP/IP hiện tại của bạn, bao gồm địa chỉ của bạn, địa chỉ máy chủ DNS, loại bộ điều hợp, và nhiều thông tin khác. Ví dụ, bạn có thể thu thập tất cả những thông tin này về máy chủ của bạn chỉ bằng cách nhập lệnh:

ipconfig /all

vào Command Prompt, như được minh họa trong ảnh chụp màn hình bên dưới.



```
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. All rights reserved.

D:\Workspaces>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-26T57VF
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : lan

Unknown adapter Local Area Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : TeamViewer VPN Adapter
Physical Address. . . . . : 00-FF-F9-41-D0-09
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address. . . . . : 00-93-37-DB-97-B0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

ipconfig cũng rất hữu ích trong việc quản lý thông tin DNS được lưu trữ trên máy chủ của bạn. Trong Section 2.5, chúng ta đã học rằng một máy chủ có thể lưu các bản ghi DNS mà nó đã nhận gần đây. Để xem những bản ghi DNS được lưu trong bộ nhớ cache này, sau dấu nhắc lệnh C:>, nhập lệnh sau:

ipconfig /displaydns


```

D:\Workspaces>ipconfig /displaydns

Windows IP Configuration

telemetry-incoming.r53-2.services.mozilla.com
-----
Record Name . . . . . : telemetry-incoming.r53-2.services.mozilla.com
Record Type . . . . . : 1
Time To Live . . . . . : 1944
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 34.120.208.123


spocs.getpocket.com
-----
Record Name . . . . . : spocs.getpocket.com
Record Type . . . . . : 5
Time To Live . . . . . : 38
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : prod.ads.prod.webservices.mozgcp.net


Record Name . . . . . : prod.ads.prod.webservices.mozgcp.net
Record Type . . . . . : 1
Time To Live . . . . . : 38
Data Length . . . . . : 4
Section . . . . . : Answer

```

Trong hình trên, ta có:

- telemetry-incoming.r53-2.services.mozilla.com: Đây là một bản ghi A với địa chỉ IP là 34.120.208.123. Thời gian TTL của bản ghi này là 1944 giây trước khi nó hết hạn và cần được làm mới.
- spocs.getpocket.com: Đây là một bản ghi CNAME (Canonical Name) liên kết với prod.ads.prod.webservices.mozgcp.net. Bản ghi này cũng có một thời gian TTL, và hệ thống sẽ giữ nó trong khoảng 30 giây trước khi cần làm mới.

Mỗi bản ghi sẽ hiển thị thời gian còn lại của **Time to Live (TTL)** tính bằng giây. Để xóa bộ nhớ cache này, hãy nhập lệnh:

```
ipconfig /flushdns
```

Lệnh này sẽ xóa sạch tất cả các bản ghi trong bộ nhớ cache và nạp lại các bản ghi từ tệp **hosts**.

```

D:\Workspaces>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

```

3. Tracing DNS with Wireshark

Bây giờ chúng ta đã quen thuộc với *nslookup* và *ipconfig*, hãy bắt đầu tiến hành một số việc nghiêm túc. Hãy cùng bắt đầu việc bắt các gói tin DNS được tạo ra bởi hoạt động lướt web thông thường.

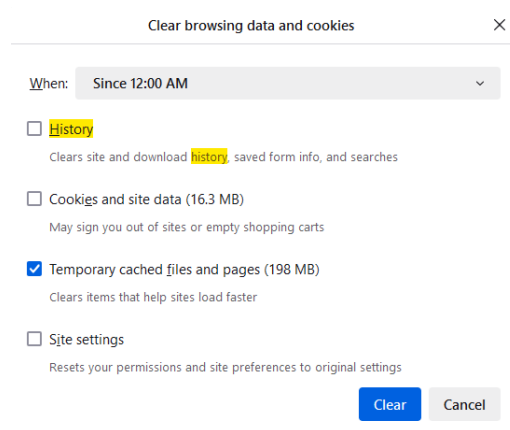
1. Sử dụng *ipconfig* để xóa bộ nhớ cache DNS trên máy của bạn.

```
D:\Workspaces>ipconfig /flushdns

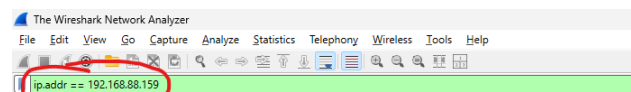
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

2. Mở trình duyệt và xóa bộ nhớ cache của trình duyệt. (Với Internet Explorer, vào menu Tools và chọn Internet Options; sau đó ở tab General, chọn Delete Files.)

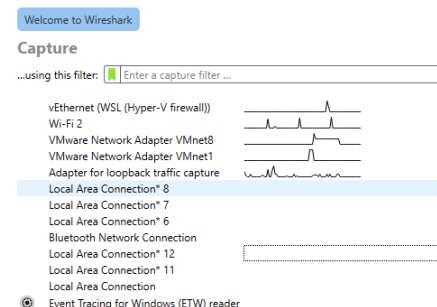


3. Mở Wireshark và nhập `ip.addr == your_IP_address` vào bộ lọc, nơi bạn có thể lấy địa chỉ IP của mình bằng *ipconfig*. Bộ lọc này sẽ loại bỏ tất cả các gói tin không có nguồn gốc hoặc không phải là đích đến của máy của bạn.

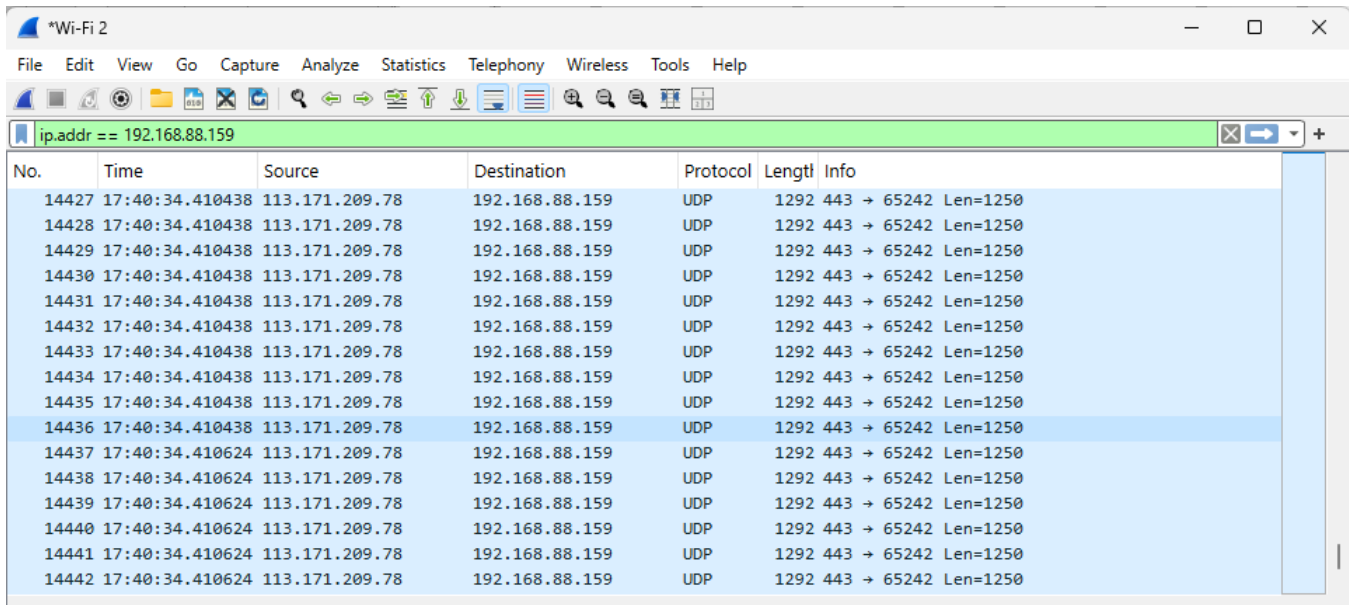


```
Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . : lan
Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%21
IPv4 Address. . . . . : 192.168.88.159
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.88.1
```

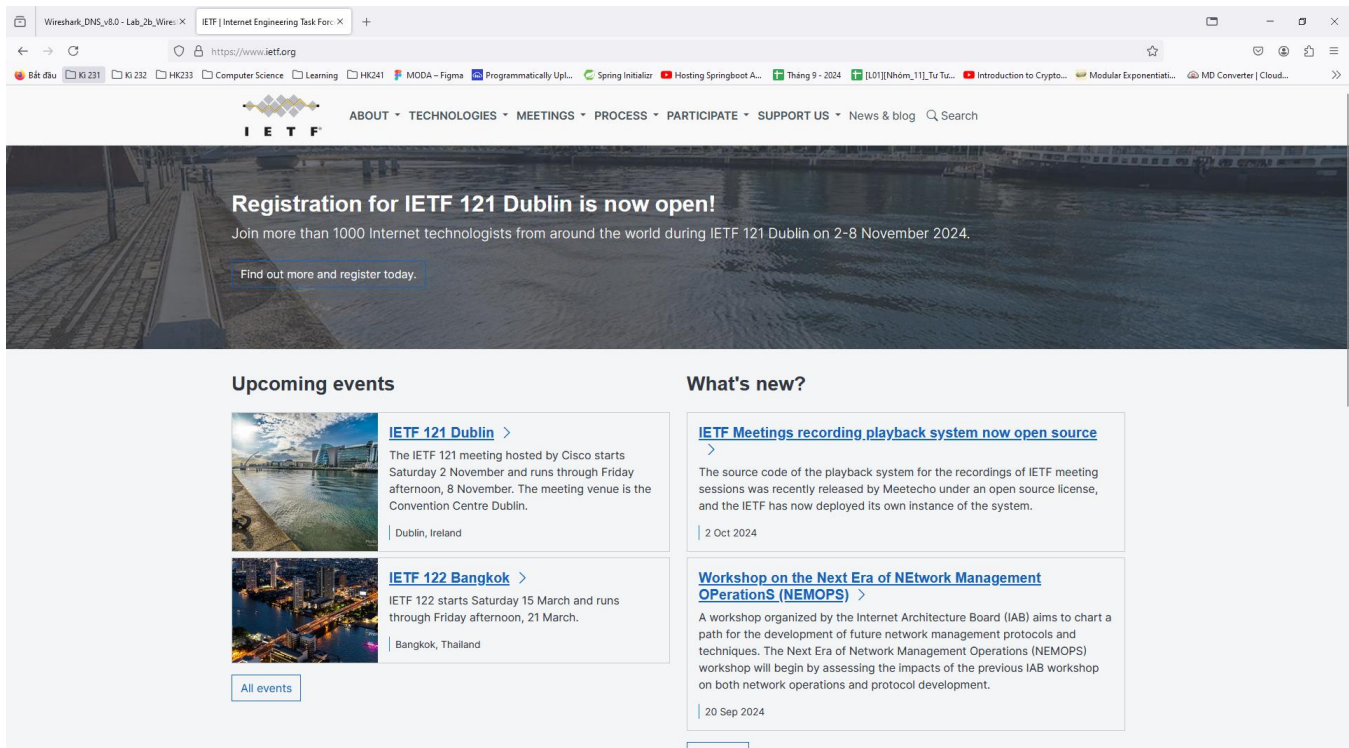


4. Bắt đầu việc bắt gói tin trong Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
14427	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14428	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14429	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14430	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14431	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14432	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14433	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14434	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14435	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14436	17:40:34.410438	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14437	17:40:34.410624	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14438	17:40:34.410624	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14439	17:40:34.410624	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14440	17:40:34.410624	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14441	17:40:34.410624	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250
14442	17:40:34.410624	113.171.209.78	192.168.88.159	UDP	1292	443 → 65242 Len=1250

5. Trong trình duyệt của bạn, truy cập trang web: <http://www.ietf.org>.



Registration for IETF 121 Dublin is now open!
Join more than 1000 Internet technologists from around the world during IETF 121 Dublin on 2-8 November 2024.
[Find out more and register today.](#)

Upcoming events

- IETF 121 Dublin**
The IETF 121 meeting hosted by Cisco starts Saturday 2 November and runs through Friday afternoon, 8 November. The meeting venue is the Convention Centre Dublin.
Dublin, Ireland
- IETF 122 Bangkok**
IETF 122 starts Saturday 15 March and runs through Friday afternoon, 21 March.
Bangkok, Thailand

[All events](#)

What's new?

- IETF Meetings recording playback system now open source**
The source code of the playback system for the recordings of IETF meeting sessions was recently released by Meetecho under an open source license, and the IETF has now deployed its own instance of the system.
2 Oct 2024
- Workshop on the Next Era of Network Management OperationS (NEMOPS)**
A workshop organized by the Internet Architecture Board (IAB) aims to chart a path for the development of future network management protocols and techniques. The Next Era of Network Management Operations (NEMOPS) workshop will begin by assessing the impacts of the previous IAB workshop on both network operations and protocol development.
20 Sep 2024

[All news](#)

6. Dừng việc bắt gói tin.

Nếu bạn không thể chạy Wireshark trên một kết nối mạng trực tiếp, bạn có thể tải xuống tệp theo dấu gói tin được ghi lại khi thực hiện các bước trên trên một trong những máy tính của

tác giả. Trả lời các câu hỏi dưới đây. Bất cứ khi nào có thể, khi trả lời câu hỏi, bạn nên nộp một bản in của gói tin (hoặc các gói tin) mà bạn đã sử dụng để trả lời câu hỏi được yêu cầu. Ghi chú vào bản in để giải thích câu trả lời của bạn. Để in một gói tin, hãy sử dụng File->Print, chọn Selected packet only, chọn Packet summary line, và chọn số lượng thông tin gói tin tối thiểu cần thiết để trả lời câu hỏi.

Trả lời câu hỏi

4. Xác định các tin nhắn truy vấn và phản hồi DNS. Chúng được gửi qua UDP hay TCP?

No.	Time	Source	Destination	Protocol	Length	Info
64	17:40:12.181196	192.168.88.159	192.168.88.1	DNS	68	Standard query 0xc9dd A wpad.lan
65	17:40:12.184127	192.168.88.1	192.168.88.159	DNS	68	Standard query response 0xc9dd No such name A wpad.lan
6328	17:40:18.660066	192.168.88.159	192.168.88.1	DNS	84	Standard query 0x1ebc HTTPS www.ietf.org
6330	17:40:18.660099	192.168.88.159	192.168.88.1	DNS	84	Standard query 0x9964 A www.ietf.org
6335	17:40:18.675549	192.168.88.1	192.168.88.159	DNS	118	Standard query response 0x9964 A www.ietf.org A 104.16.45.99 A 104.16.44.99
6342	17:40:18.711271	192.168.88.1	192.168.88.159	DNS	159	Standard query response 0x1ebc HTTPS www.ietf.org HTTPS
6413	17:40:26.406157	192.168.88.159	192.168.88.1	DNS	74	Standard query 0x2629 A www.google.com
6414	17:40:26.408628	192.168.88.1	192.168.88.159	DNS	90	Standard query response 0x2629 A www.google.com A 142.250.76.228
6415	17:40:26.409647	192.168.88.159	192.168.88.1	DNS	74	Standard query 0x5a9f AAAA www.google.com
6417	17:40:26.417259	192.168.88.1	192.168.88.159	DNS	102	Standard query response 0x5a9f AAAA www.google.com AAAA 2404:6800:4005:819::2004
6459	17:40:27.314499	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xefcb HTTPS www.ietf.org
6460	17:40:27.314499	192.168.88.1	192.168.88.159	DNS	72	Standard query 0xf5f4 A www.ietf.org
6461	17:40:27.348638	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xefcb HTTPS www.ietf.org
6462	17:40:27.348693	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xf5f4 A www.ietf.org
6464	17:40:27.429694	192.168.88.1	192.168.88.159	DNS	145	Standard query response 0xefcb HTTPS www.ietf.org HTTPS
6465	17:40:27.429694	192.168.88.1	192.168.88.159	DNS	104	Standard query response 0xf5f4 A www.ietf.org A 104.16.44.99 A 104.16.45.99
6466	17:40:27.429694	192.168.88.1	192.168.88.159	DNS	104	Standard query response 0xf5f4 A www.ietf.org A 104.16.45.99 A 104.16.44.99

Transmission Control Protocol, Src Port: 53, Dst Port: 65299, Seq: 1, Ack: 33, Len: 64

Source Port: 53
Destination Port: 65299
[Stream index: 6]
[Stream Packet Number: 8]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 64]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3759218670
[Next Sequence Number: 65 (relative sequence number)]
Acknowledgment Number: 33 (relative ack number)
Acknowledgment number (raw): 133506661
0101 ... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 913
[Calculated window size: 14608]
[Window size scaling factor: 16]
Checksum: 0x644e [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (64 bytes)
[PDU Size: 64]

User Datagram Protocol, Src Port: 53, Dst Port: 59249

Source Port: 53
Destination Port: 59249
Length: 70
Checksum: 0xa26c [unverified]
[Checksum Status: Unverified]
[Stream index: 32]
[Stream Packet Number: 3]
[Timestamps]
[Time since first frame: 0.115195000 seconds]
[Time since previous frame: 0.081001000 seconds]
UDP payload (62 bytes)

Các tin nhắn DNS có thể được gửi qua cả hai giao thức: UDP và TCP. Trong danh sách gói tin mà em đã thu thập, có cả gói tin sử dụng UDP và TCP. Ta có thể nhận ra điều này từ các chi tiết của mỗi gói.

- Gói tin sử dụng TCP (gói No.6335): Ví dụ như gói tin với Source Port: 53, Destination Port: 65299 (hình bên trái). Dấu hiệu là tiêu đề có ghi Transmission Control Protocol (TCP) và các thông số đi kèm như sequence number, acknowledgment number.

- Gói tin sử dụng UDP (gói No.6465): Ví dụ như gói tin với Source Port: 53, Destination Port: 59249 (hình bên phải). Dấu hiệu là tiêu đề có ghi User Datagram Protocol (UDP) và thông số đơn giản hơn, không có sequence hoặc acknowledgment number.

Như vậy các tin nhắn DNS được gửi qua cả UDP và TCP, tùy thuộc vào kích thước và yêu cầu cụ thể của mỗi gói tin.

5. Địa chỉ cổng đích cho tin nhắn truy vấn DNS là gì? Địa chỉ cổng nguồn của tin nhắn phản hồi DNS là gì?

No.	Time	Source	Destination	Protocol	Length	Info
6328	17:40:18.660066	192.168.88.159	192.168.88.1	DNS	84	Standard query 0x1ebc HTTPS www.ietf.org

```

Transmission Control Protocol, Src Port: 65300, Dst Port: 53, Seq: 3, Ack: 1, Len: 30
  Source Port: 65300
  Destination Port: 53
  [Stream index: 7]
  [Stream Packet Number: 5]
  [Conversation completeness: Complete, WITH_DATA (63)]
  [TCP Segment Len: 30]
  Sequence Number: 3 (relative sequence number)
  Sequence Number (raw): 3514110985
  [Next Sequence Number: 33 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1555708273
  0101 ... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH, ACK)
  Window: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
  Checksum: 0x322a [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (30 bytes)
  [PDU Size: 32]
  TCP segment data (30 bytes)
[2 Reassembled TCP Segments (32 bytes): #6327(2), #6328(30)]

```

Đối với tin nhắn truy vấn (source là IP máy ta và destination là máy chủ ta truy vấn), cổng đích là: Port 53 trên máy chủ DNS; cổng nguồn là một cổng ngẫu nhiên: Port 65300.

Khi phản hồi DNS được trả về, cổng nguồn là Port 53, và cổng đích là cổng ngẫu nhiên được sử dụng bởi truy vấn ban đầu (Port 65299).

6. Tin nhắn truy vấn DNS được gửi tới địa chỉ IP nào? Sử dụng *ipconfig* để xác định địa chỉ IP của máy chủ DNS cục bộ của bạn. Hai địa chỉ IP này có giống nhau không?

No.	Time	Source	Destination	Protocol	Length	Info
6328	17:40:18.660066	192.168.88.159	192.168.88.1	DNS	84	Standard query 0x1ebc HTTPS www.ietf.org

```

Wireless LAN adapter Wi-Fi 2:
  Connection-specific DNS Suffix . : lan
  Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
  Physical Address. . . . . : 08-93-37-DB-97-AF
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%21(Preferred)
  IPv4 Address. . . . . : 192.168.88.159(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Sunday, October 6, 2024 11:48:46 AM
  Lease Expires . . . . . : Wednesday, October 9, 2024 3:35:08 AM
  Default Gateway . . . . . : 192.168.88.1
  DHCP Server . . . . . : 192.168.88.1
  DHCPv6 IAID . . . . . : 620794679
  DHCPv6 Client DUID. . . . . : 08-01-00-01-2E-32-CA-37-00-93-37-DB-97-AF
  DNS Servers . . . . . : 192.168.88.1
  NetBIOS over Tcpip. . . . . : Enabled

```

Như hình ảnh bên cạnh, DNS cục bộ có địa chỉ IP là 192.168.88.1, có giá trị bằng giá trị của cột Destination IP trong các packet truy vấn, tức là truy vấn DNS đã được gửi đến máy chủ DNS cục bộ của em.

7. Kiểm tra tin nhắn truy vấn DNS. "Loại" (Type) của truy vấn DNS là gì? Tin nhắn truy vấn có chứa bất kỳ "câu trả lời" nào không?

Tìm gói tin có Protocol là DNS trong danh sách gói đã bắt, chọn một gói tin có thông tin "Standard query" trong cột Info. Sau khi chọn gói tin DNS, mở rộng phần Domain Name System (query) trong phần chi tiết của gói tin.

Tìm trường Type trong tin nhắn truy vấn. Trường này sẽ cho biết loại truy vấn DNS, chẳng hạn như:

- A: Địa chỉ IPv4 (truy vấn tìm địa chỉ IP của một tên miền).
- AAAA: Địa chỉ IPv6.
- MX: Truy vấn mail exchange (máy chủ thư).
- CNAME: Tên miền bí danh.

```
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Destination: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Source: Intel_db:97:af (00:93:37:db:97:af)
Type: IPv4 (0x0800)
[Stream index: 9]
```

Trong ví dụ trên, em lựa chọn gói 6335, có trường Type: Ipv4, tức là truy vấn tìm địa chỉ IP của một tên miền.

Trong các tin nhắn truy vấn DNS, ta sẽ không thấy bất kỳ "câu trả lời" nào, vì nó chỉ đang gửi yêu cầu tới máy chủ DNS để lấy thông tin. Thông thường, các "câu trả lời" chỉ xuất hiện trong gói tin phản hồi DNS (DNS response), không có trong gói truy vấn.

8. Kiểm tra tin nhắn phản hồi DNS. Có bao nhiêu "câu trả lời" được cung cấp? Mỗi câu trả lời chứa những gì?

Trong ví dụ này, em chọn gói tin phản hồi 6465, Answer RRs: 2 cho biết có hai "câu trả lời" (RR - Resource Records) trong phản hồi này.

```
Domain Name System (response)
Length: 62
Transaction ID: 0x9964
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
Answers
[Request In: 6330]
[Time: 0.015450000 seconds]
```


No.	Time	Source	Destination	Protocol	Length	Info
6335	17:40:18.675549	192.168.88.1	192.168.88.159	DNS	118	Standard query response 0x9964 A www.ietf.org A 104.16.45.99 A 104.16.44.99

Cụ thể, dòng Standard query response 0x9964 A www.ietf.org A có nghĩa là:

- Standard query response 0x9964 A www.ietf.org A: Đây là phản hồi cho truy vấn DNS yêu cầu địa chỉ IP của tên miền www.ietf.org. Truy vấn này thuộc loại A, tức là tìm địa chỉ IP dạng IPv4.
- 104.16.45.99 A 104.16.44.99: Đây là hai địa chỉ IP trong phản hồi của máy chủ DNS. Điều này có nghĩa là máy chủ DNS đã trả về hai địa chỉ IP khác nhau cho tên miền www.ietf.org. Máy chủ www.ietf.org có thể được lưu trữ trên nhiều máy chủ khác nhau, và các địa chỉ IP này được dùng để liên kết với máy chủ của trang web đó.

9. Xem xét gói TCP SYN tiếp theo được gửi bởi máy của bạn. Địa chỉ IP đích của gói SYN này có tương ứng với bất kỳ địa chỉ IP nào được cung cấp trong tin nhắn phản hồi DNS không?

Trong Wireshark, gói TCP SYN thường có Protocol là TCP và Info sẽ chứa từ "SYN". Đây là gói đầu tiên trong quá trình bắt tay 3 bước TCP (TCP 3-way handshake).

No.	Time	Source	Destination	Protocol	Length	Info
6288	17:40:15.434874	13.69.116.108	192.168.88.159	TLSv1.2	93	Application Data
6289	17:40:15.488486	192.168.88.159	13.69.116.108	TCP	54	65248 → 443 [ACK] Seq=1032 Ack=40 Win=516 Len=0
6290	17:40:15.689173	13.69.116.108	192.168.88.159	TLSv1.2	148	Application Data
6291	17:40:15.690028	192.168.88.159	13.69.116.108	TLSv1.2	89	Application Data
6292	17:40:15.960601	13.69.116.108	192.168.88.159	TCP	60	443 → 65248 [ACK] Seq=134 Ack=1067 Win=16381 Len=0
6293	17:40:16.078052	192.168.88.159	20.187.186.89	TCP	55	63857 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1
6294	17:40:16.112658	20.187.186.89	192.168.88.159	TCP	66	443 → 63857 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
6295	17:40:16.388737	192.168.88.159	113.171.234.34	TCP	55	65280 → 80 [ACK] Seq=1 Ack=1 Win=509 Len=1
6296	17:40:16.394886	113.171.234.34	192.168.88.159	TCP	66	80 → 65280 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
6297	17:40:16.403612	192.168.88.159	113.171.234.34	TCP	55	65281 → 80 [ACK] Seq=1 Ack=1 Win=509 Len=1
6298	17:40:16.698497	192.168.88.159	13.69.116.108	TLSv1.2	134	Application Data
6299	17:40:16.698564	192.168.88.159	13.69.116.108	TLSv1.2	887	Application Data
6302	17:40:16.900263	13.69.116.108	192.168.88.159	TCP	60	443 → 65248 [ACK] Seq=134 Ack=1980 Win=16386 Len=0
6303	17:40:16.913998	13.69.116.108	192.168.88.159	TLSv1.2	148	Application Data
6304	17:40:16.963596	192.168.88.159	13.69.116.108	TCP	54	65248 → 443 [ACK] Seq=1980 Ack=228 Win=515 Len=0
6305	17:40:17.413738	192.168.88.159	113.171.234.34	TCP	55	[TCP Keep-Alive] 65281 → 80 [ACK] Seq=1 Ack=1 Win=509 Len=1
6306	17:40:17.417587	113.171.234.34	192.168.88.159	TCP	66	80 → 65281 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
6319	17:40:18.486201	162.159.130.234	192.168.88.159	TLSv1.2	125	Application Data
6320	17:40:18.531957	192.168.88.159	162.159.130.234	TCP	54	64843 → 443 [ACK] Seq=1 Ack=72 Win=509 Len=0
6321	17:40:18.658003	192.168.88.159	192.168.88.1	TCP	66	65299 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6322	17:40:18.658122	192.168.88.159	192.168.88.1	TCP	66	65300 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6323	17:40:18.659776	192.168.88.1	192.168.88.159	TCP	66	53 → 65299 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
6324	17:40:18.659776	192.168.88.1	192.168.88.159	TCP	66	53 → 65300 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16

Em sử dụng gói 6321, có IP của Destination như sau:

No.	Time	Source	Destination	Protocol	Length	Info
6321	17:40:18.658003	192.168.88.159	192.168.88.1	TCP	66	65299 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Như vậy, gói TCP SYN này không gửi tới địa chỉ IP nào được cung cấp trong tin nhắn phản hồi DNS (104.16.45.99 hoặc 104.16.44.99). Gói SYN này có lẽ liên quan đến một kết nối khác, không phải kết nối đến www.ietf.org.

10. Trang web này có chứa hình ảnh. Trước khi truy xuất từng hình ảnh, máy của bạn có phát hành các truy vấn DNS mới không?

Trong Wireshark, lọc các gói DNS (bằng cách sử dụng bộ lọc như dns), sau đó tìm các truy vấn DNS mới được gửi sau khi trang web ban đầu được tải, đặc biệt là sau khi các gói tin đầu tiên được tải. Nếu trang web có chứa hình ảnh từ các tên miền khác với tên miền của trang chính (www.ietf.org), sẽ có thêm truy vấn DNS cho những tên miền đó. Nếu các truy vấn này xuất hiện, điều này có nghĩa là máy tính đã gửi các truy vấn DNS mới để tải hình ảnh.

No.	Time	Source	Destination	Protocol	Length	Info
64	17:40:12.181196	192.168.88.159	192.168.88.1	DNS	68	Standard query 0xc9dd A wpad.lan
65	17:40:12.184127	192.168.88.1	192.168.88.159	DNS	68	Standard query response 0xc9dd No such name A wpad.lan
6328	17:40:18.660066	192.168.88.159	192.168.88.1	DNS	84	Standard query 0x1ebc HTTPS www.ietf.org
6330	17:40:18.660099	192.168.88.159	192.168.88.1	DNS	84	Standard query 0x9964 A www.ietf.org
6335	17:40:18.675549	192.168.88.1	192.168.88.159	DNS	118	Standard query response 0x9964 A www.ietf.org A 104.16.45.99 A 104.16.44.99
6342	17:40:18.711271	192.168.88.1	192.168.88.159	DNS	159	Standard query response 0x1ebc HTTPS www.ietf.org HTTPS
6413	17:40:26.406157	192.168.88.159	192.168.88.1	DNS	74	Standard query 0x2629 A www.google.com
6414	17:40:26.408628	192.168.88.1	192.168.88.159	DNS	90	Standard query response 0x2629 A www.google.com A 142.250.76.228
6415	17:40:26.409647	192.168.88.159	192.168.88.1	DNS	74	Standard query 0x5a9f AAAA www.google.com
6417	17:40:26.417259	192.168.88.1	192.168.88.159	DNS	102	Standard query response 0x5a9f AAAA www.google.com AAAA 2404:6800:4005:819::2004
6459	17:40:27.314499	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xfcb HTTPS www.ietf.org
6460	17:40:27.314499	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xf5f4 A www.ietf.org
6461	17:40:27.348638	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xfcb HTTPS www.ietf.org
6462	17:40:27.348693	192.168.88.159	192.168.88.1	DNS	72	Standard query 0xf5f4 A www.ietf.org
6464	17:40:27.429694	192.168.88.1	192.168.88.159	DNS	145	Standard query response 0xfcb HTTPS www.ietf.org HTTPS
6465	17:40:27.429694	192.168.88.1	192.168.88.159	DNS	104	Standard query response 0xf5f4 A www.ietf.org A 104.16.44.99 A 104.16.45.99
6466	17:40:27.429694	192.168.88.1	192.168.88.159	DNS	104	Standard query response 0xf5f4 A www.ietf.org A 104.16.45.99 A 104.16.44.99
6468	17:40:27.430887	192.168.88.159	192.168.88.1	DNS	72	Standard query 0x4163 A www.ietf.org
6469	17:40:27.435519	192.168.88.1	192.168.88.159	DNS	145	Standard query response 0xfcb HTTPS www.ietf.org HTTPS
6470	17:40:27.435519	192.168.88.1	192.168.88.159	DNS	104	Standard query response 0x4163 A www.ietf.org A 104.16.44.99 A 104.16.45.99
6471	17:40:27.435888	192.168.88.159	192.168.88.1	DNS	72	Standard query 0x53a8 AAAA www.ietf.org
6473	17:40:27.472877	192.168.88.159	192.168.88.1	DNS	72	Standard query 0x53a8 AAAA www.ietf.org
6477	17:40:27.502389	192.168.88.1	192.168.88.159	DNS	128	Standard query response 0x53a8 AAAA www.ietf.org AAAA 2606:4700::6810:2c63 AAAA 2606:4700::6810:2d63
6478	17:40:27.502389	192.168.88.1	192.168.88.159	DNS	128	Standard query response 0x53a8 AAAA www.ietf.org AAAA 2606:4700::6810:2d63 AAAA 2606:4700::6810:2c63
6520	17:40:27.775227	192.168.88.159	192.168.88.1	DNS	75	Standard query 0x11e4 A static.ietf.org

Dựa trên các gói DNS em đã thu thập được, có thể thấy rằng trước khi truy xuất từng hình ảnh, máy của em đã phát hành các truy vấn DNS mới. Cụ thể, mỗi khi trình duyệt cần tải một hình ảnh hoặc tài nguyên từ các miền khác, em thấy các truy vấn DNS mới được gửi đi để phân giải tên miền của máy chủ chứa những tài nguyên đó. Trong danh sách gói tin, có thể thấy các truy vấn liên quan đến các tài nguyên như analytics.ietf.org, static.ietf.org, và static.ietf.org HTTPS, với nhiều truy vấn khác nhau cho mỗi tài nguyên.

Như vậy, trước khi tải hình ảnh, trình duyệt của em đã gửi thêm truy vấn DNS để lấy địa chỉ IP của các máy chủ chứa các hình ảnh và tài nguyên những. Vậy nên câu trả lời là **CÓ**, máy của em đã phát hành các truy vấn DNS mới trước khi truy xuất từng hình ảnh từ trang web.

Bây giờ hãy thử chơi với nslookup

- Bắt đầu việc bắt gói tin
- Thực hiện một lệnh nslookup trên www.mit.edu
- Dừng việc bắt gói tin

No.	Time	Source	Destination	Protocol	Length	Info
1549	20:25:55.620513	192.168.88.159	192.168.88.1	DNS	115	Standard query 0xe8c1 A turing-writingassistance.edge.microsoft.com
1551	20:25:55.620560	192.168.88.159	192.168.88.1	DNS	115	Standard query 0x4553 HTTPS turing-writingassistance.edge.microsoft.com
1558	20:25:55.643349	192.168.88.1	192.168.88.159	DNS	255	Standard query response 0x4553 HTTPS turing-writingassistance.edge.microsoft.com CNAME turing-writingassistance.edge.microsoft.com.b-0005.b-msedg
1559	20:25:55.643349	192.168.88.1	192.168.88.159	DNS	224	Standard query response 0xe8c1 A turing-writingassistance.edge.microsoft.com CNAME turing-writingassistance.edge.microsoft.com.b-0005.b-msedg
1860	20:26:00.702157	192.168.88.159	192.168.88.1	DNS	86	Standard query 0x3ee9 A ab.chatgpt.com
1864	20:26:00.708240	192.168.88.159	192.168.88.1	DNS	86	Standard query 0x77ef HTTPS ab.chatgpt.com
1874	20:26:00.737937	192.168.88.1	192.168.88.159	DNS	158	Standard query response 0x77ef HTTPS ab.chatgpt.com HTTPS
1876	20:26:00.738329	192.168.88.1	192.168.88.159	DNS	120	Standard query response 0x3ee9 A ab.chatgpt.com A 172.64.155.209 A 104.18.32.47
2645	20:26:09.189979	192.168.88.159	192.168.88.1	DNS	74	Standard query 0xc17a A www.google.com
2647	20:26:09.190394	192.168.88.1	192.168.88.159	DNS	90	Standard query response 0xc17a A www.google.com A 142.250.197.36
2785	20:26:10.991269	192.168.88.159	192.168.88.1	DNS	92	Standard query 0xcce4 HTTPS accounts.youtube.com
2787	20:26:10.991305	192.168.88.159	192.168.88.1	DNS	92	Standard query 0x5c98 A accounts.youtube.com
2792	20:26:11.014270	192.168.88.1	192.168.88.159	DNS	138	Standard query response 0x5c98 A accounts.youtube.com CNAME www3.l.google.com A 142.250.71.174
2794	20:26:11.015645	192.168.88.1	192.168.88.159	DNS	172	Standard query response 0xcce4 HTTPS accounts.youtube.com CNAME www3.l.google.com SOA ns1.google.com
3742	20:26:20.748878	192.168.88.159	192.168.88.1	DNS	96	Standard query 0x564f HTTPS www.google-analytics.com
3744	20:26:20.748946	192.168.88.159	192.168.88.1	DNS	96	Standard query 0x564f HTTPS www.google-analytics.com
3751	20:26:20.762314	192.168.88.1	192.168.88.159	DNS	155	Standard query response 0x564f HTTPS www.google-analytics.com SOA ns1.google.com
3752	20:26:20.762314	192.168.88.1	192.168.88.159	DNS	114	Standard query response 0xe5a6 A www.google-analytics.com A 142.250.71.206
3776	20:26:20.808297	192.168.88.159	192.168.88.1	DNS	108	Standard query 0xbcc8 A functional.events.data.microsoft.com
3778	20:26:20.808349	192.168.88.159	192.168.88.1	DNS	108	Standard query 0x3582 HTTPS functional.events.data.microsoft.com
3798	20:26:20.828235	192.168.88.1	192.168.88.159	DNS	282	Standard query response 0x3582 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedcolprdcu
3804	20:26:20.840667	192.168.88.1	192.168.88.159	DNS	240	Standard query response 0x8cc8 A functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedcolprdcu20
4649	20:26:25.879838	192.168.88.159	192.168.88.1	DNS	86	Standard query 0xb421 A t-ring-fallback.msedge.net
4650	20:26:25.885996	192.168.88.1	192.168.88.159	DNS	156	Standard query response 0xb421 A t-ring-fallback.msedge.net CNAME t-ring-t-9999.fb-t-msedge.net CNAME t-9999.fb-t-msedge.net A 13.107.253.254
4686	20:26:26.038170	192.168.88.159	192.168.88.1	DNS	79	Standard query 0x5065 A t-ring-t.msedge.net
4687	20:26:26.043779	192.168.88.1	192.168.88.159	DNS	153	Standard query response 0x5065 A t-ring-t.msedge.net CNAME t-ring-s-part-t-9999.t-msedge.net CNAME s-part-t-9999.t-msedge.net A 13.107.246.254

Chúng ta thấy từ ảnh chụp màn hình trên rằng **nslookup** thực sự đã gửi ba truy vấn DNS và nhận được ba phản hồi DNS. Để phục vụ cho bài tập này, khi trả lời các câu hỏi dưới đây, hãy bỏ qua hai bộ truy vấn/phản hồi đầu tiên, vì chúng dành riêng cho **nslookup** và không được tạo ra bình thường bởi các ứng dụng Internet tiêu chuẩn. Bạn nên tập trung vào truy vấn và tin nhắn phản hồi cuối cùng.

Trả lời câu hỏi

11. Công đích cho tin nhắn truy vấn DNS là gì? Công nguồn của tin nhắn phản hồi DNS là gì?

No.	Time	Source	Destination	Protocol	Length	Info
2645	20:26:09.189979	192.168.88.159	192.168.88.1	DNS	74	Standard query 0xc17a A www.google.com
2647	20:26:09.190394	192.168.88.1	192.168.88.159	DNS	90	Standard query response 0xc17a A www.google.com A 142.250.197.36
2785	20:26:10.991269	192.168.88.159	192.168.88.1	DNS	92	Standard query 0xcce4 HTTPS accounts.youtube.com
2787	20:26:10.991305	192.168.88.159	192.168.88.1	DNS	92	Standard query 0x5c98 A accounts.youtube.com
2792	20:26:11.014270	192.168.88.1	192.168.88.159	DNS	138	Standard query response 0x5c98 A accounts.youtube.com CNAME www3.l.google.com A 142.250.71.174
2794	20:26:11.015645	192.168.88.1	192.168.88.159	DNS	172	Standard query response 0xcce4 HTTPS accounts.youtube.com CNAME www3.l.google.com SOA ns1.google.com
3742	20:26:20.748878	192.168.88.159	192.168.88.1	DNS	96	Standard query 0x564f HTTPS www.google-analytics.com
3744	20:26:20.748946	192.168.88.159	192.168.88.1	DNS	96	Standard query 0x564f HTTPS www.google-analytics.com
3751	20:26:20.762314	192.168.88.1	192.168.88.159	DNS	155	Standard query response 0x564f HTTPS www.google-analytics.com SOA ns1.google.com
3752	20:26:20.762314	192.168.88.1	192.168.88.159	DNS	114	Standard query response 0xe5a6 A www.google-analytics.com A 142.250.71.206
3776	20:26:20.808297	192.168.88.159	192.168.88.1	DNS	108	Standard query 0xbcc8 A functional.events.data.microsoft.com
3778	20:26:20.808349	192.168.88.159	192.168.88.1	DNS	108	Standard query 0x3582 HTTPS functional.events.data.microsoft.com
3798	20:26:20.828235	192.168.88.1	192.168.88.159	DNS	282	Standard query response 0x3582 HTTPS functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedcolprdcu00.eastus.cloudapp.azure.com SOA ..
3804	20:26:20.840667	192.168.88.1	192.168.88.159	DNS	240	Standard query response 0x8cc8 A functional.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedcolprdcu20.centralus.cloudapp.azure.com A 104..
4649	20:26:25.879838	192.168.88.159	192.168.88.1	DNS	86	Standard query 0xb421 A t-ring-fallback.msedge.net
4650	20:26:25.885996	192.168.88.1	192.168.88.159	DNS	156	Standard query response 0xb421 A t-ring-fallback.msedge.net CNAME t-ring-t-9999.fb-t-msedge.net CNAME t-9999.fb-t-msedge.net A 13.107.253.254
4686	20:26:26.038170	192.168.88.159	192.168.88.1	DNS	79	Standard query 0x5065 A t-ring-t.msedge.net
4687	20:26:26.043779	192.168.88.1	192.168.88.159	DNS	153	Standard query response 0x5065 A t-ring-t.msedge.net CNAME t-ring-s-part-t-9999.t-msedge.net CNAME s-part-t-9999.t-msedge.net A 13.107.246.254
4721	20:26:26.110112	192.168.88.159	192.168.88.1	DNS	113	Standard query 0x22f5 A 01379f84e7ac49585a5d64812b467.clo.fortprintdns.com
4724	20:26:26.136275	192.168.88.1	192.168.88.159	DNS	245	Standard query response 0x22f5 A 01379f84e7ac49585a5d64812b467.clo.fortprintdns.com CNAME a-ring-ipv6only.msedge.net CNAME ipv6-a-9999-a.msedge.net SOA ns1-a.msedge.net
5118	20:26:27.278027	192.168.88.159	192.168.88.1	DNS	89	Standard query 0x36d2 A cdn.olistic.com
5122	20:26:27.278247	192.168.88.159	192.168.88.1	DNS	89	Standard query 0xc433 HTTPS cdn.olistic.com
5118	20:26:27.292804	192.168.88.1	192.168.88.159	DNS	164	Standard query response 0xc433 HTTPS cdn.olistic.com HTTPS
5119	20:26:27.292804	192.168.88.1	192.168.88.159	DNS	123	Standard query response 0x36d2 A cdn.olistic.com A 172.64.146.98 A 104.18.41.158
5407	20:26:30.021150	192.168.88.159	192.168.88.1	DNS	100	Standard query 0xc210 A browser-intake-datadoghq.com
5411	20:26:30.023400	192.168.88.159	192.168.88.1	DNS	100	Standard query 0x4724 HTTPS browser-intake-datadoghq.com
5416	20:26:30.036102	192.168.88.1	192.168.88.159	DNS	287	Standard query response 0xe210 A browser-intake-datadoghq.com A 3.233.158.25 A 3.233.158.24 A 3.233.158.26 NS ns-1264.awsdns-30.org NS ns-128.awsdns-16.com NS ns-1907.awsdns-46.c..
5421	20:26:30.039566	192.168.88.1	192.168.88.159	DNS	186	Standard query response 0x4724 HTTPS browser-intake-datadoghq.com SOA ns-1907.awsdns-46.co.uk
8633	20:26:41.994808	192.168.88.159	192.168.88.1	DNS	87	Standard query 0xb0c4 A play.google.com
8638	20:26:41.995848	192.168.88.159	192.168.88.1	DNS	87	Standard query 0xf408 HTTPS play.google.com
8644	20:26:42.012716	192.168.88.1	192.168.88.159	DNS	139	Standard query response 0xf408 HTTPS play.google.com SOA ns1.google.com
8645	20:26:42.012716	192.168.88.1	192.168.88.159	DNS	105	Standard query response 0xb0c4 A play.google.com A 142.250.71.238
8740	20:26:42.504913	192.168.88.159	192.168.88.1	DNS	85	Standard query 0x0005 PTR 1.88.168.192.in-addr.arpa
8741	20:26:42.507889	192.168.88.1	192.168.88.159	DNS	107	Standard query response 0x0005 PTR 1.88.168.192.in-addr.arpa PTR VMP1.jan
8742	20:26:42.508011	192.168.88.159	192.168.88.1	DNS	71	Standard query 0x0002 A www.mit.edu
8743	20:26:42.517963	192.168.88.1	192.168.88.159	DNS	110	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.ds.ch.akaedge.net A 23.66.41.81

Ở đây, em chọn gói truy vấn là gói No.8742, gói phản hồi là gói No.8743.

No.	Time	Source	Destination	Protocol	Length	Info
8742	20:26:42.508811	192.168.88.159	192.168.88.1	DNS	71	Standard query 0x0002 A www.mit.edu

User Datagram Protocol, Src Port: 65164, Dst Port: 53
Source Port: 65164
Destination Port: 53
Length: 37
Checksum: 0x3228 [unverified]
[Checksum Status: Unverified]
[Stream index: 80]
[Stream Packet Number: 1]
[Timestamps]
UDP payload (29 bytes)

Đây là gói truy vấn, với Destination Port: 53

No.	Time	Source	Destination	Protocol	Length	Info
8743	20:26:42.517963	192.168.88.1	192.168.88.159	DNS	160	Standard query response 0x0002 A www.mit.edu

User Datagram Protocol, Src Port: 53, Dst Port: 65164
Source Port: 53
Destination Port: 65164
Length: 126
Checksum: 0x32b0 [unverified]
[Checksum Status: Unverified]
[Stream index: 80]
[Stream Packet Number: 2]
[Timestamps]
UDP payload (118 bytes)

Đây là gói phản hồi, với Source Port: 53

12. Tin nhắn truy vấn DNS được gửi đến địa chỉ IP nào? Đây có phải là địa chỉ IP của máy chủ DNS cục bộ mặc định của bạn không?

Tương tự như câu hỏi số 6

No.	Time	Source	Destination	Protocol	Length	Info
8742	20:26:42.508811	192.168.88.159	192.168.88.1	DNS	71	Standard query 0x0002 A www.mit.edu

```
Wireless LAN adapter Wi-Fi 2:
Connection-specific DNS Suffix . : lan
Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . : 00-93-37-DB-97-AF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%21(Preferred)
IPv4 Address. . . . . : 192.168.88.159(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, October 6, 2024 11:48:46 AM
Lease Expires . . . . . : Wednesday, October 9, 2024 3:35:08 AM
Default Gateway . . . . . : 192.168.88.1
DHCP Server . . . . . : 192.168.88.1
DHCPv6 IAID . . . . . : 620794679
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-32-CA-37-00-93-37-DB-97-AF
DNS Servers . . . . . : 192.168.88.1
NetBIOS over Tcpip. . . . . : Enabled
```

Như hình ảnh bên cạnh, DNS cục bộ có địa chỉ IP là 192.168.88.1, có giá trị bằng giá trị của cột Destination IP trong các packet truy vấn, tức là truy vấn DNS đã được gửi đến máy chủ DNS cục bộ của em.

13. Kiểm tra tin nhắn truy vấn DNS. "Loại" (Type) của truy vấn DNS là gì? Tin nhắn truy vấn có chứa bất kỳ "câu trả lời" nào không?

Tương tự câu hỏi số 7

```
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Destination: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Source: Intel_db:97:af (00:93:37:db:97:af)
Type: IPv4 (0x0800)
[Stream index: 0]
```

Trong ví dụ trên, có trường Type: Ipv4, tức là truy vấn tìm địa chỉ IP của một tên miền.

Trong các tin nhắn truy vấn DNS, ta sẽ không thấy bất kỳ "câu trả lời" nào, vì nó chỉ đang gửi yêu cầu tới máy chủ DNS để lấy thông tin. Thông thường, các "câu trả lời" chỉ xuất hiện trong gói tin phản hồi DNS (DNS response), không có trong gói truy vấn.

14. Kiểm tra tin nhắn phản hồi DNS. Có bao nhiêu "câu trả lời" được cung cấp? Mỗi câu trả lời chứa gì?

No.	Time	Source	Destination	Protocol	Length	Info
8743	20:26:42.517963	192.168.88.1	192.168.88.159	DNS	160	Standard query response 0x0002 A www.mit.edu

```
CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.66.41.93
```

```
-----
Domain Name System (response)
Transaction ID: 0x0002
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
  www.mit.edu: type A, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Answers
[Request In: 8742]
[Time: 0.009152000 seconds]
```

Trong ví dụ này, em chọn gói tin phản hồi 6465, Answer RRs: 3 cho biết có ba "câu trả lời" (RR - Resource Records) trong phản hồi này.

15. Cung cấp một ảnh chụp màn hình

Em đã cung cấp đầy đủ ở trên.

Bây giờ lặp lại thí nghiệm trước đó, nhưng thay vào đó, thực hiện lệnh:

```
D:\Workspaces>nslookup -type=NS mit.edu
Server: VNPT.lan
Address: 192.168.88.1

Non-authoritative answer:
mit.edu nameserver = usw2.akam.net
mit.edu nameserver = ns1-173.akam.net
mit.edu nameserver = ns1-37.akam.net
mit.edu nameserver = use5.akam.net
mit.edu nameserver = use2.akam.net
mit.edu nameserver = asia1.akam.net
mit.edu nameserver = eur5.akam.net
mit.edu nameserver = asia2.akam.net
```

```
nslookup -type=NS mit.edu
```

Trả lời các câu hỏi sau

16. Tin nhắn truy vấn DNS được gửi đến địa chỉ IP nào? Đây có phải là địa chỉ IP của máy chủ DNS cục bộ mặc định của bạn không?

Ở đây, em chọn gói truy vấn là gói No.877, gói phản hồi là gói No.878.

No.	Time	Source	Destination	Protocol	Length	Info
877	20:58:22.580009	192.168.88.159	192.168.88.1	DNS	67	Standard query 0x0002 NS mit.edu

```
Wireless LAN adapter Wi-Fi 2:
Connection-specific DNS Suffix . : lan
Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . : 00-93-37-DB-97-AF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%21(Preferred)
IPv4 Address. . . . . : 192.168.88.159(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, October 6, 2024 11:48:46 AM
Lease Expires . . . . . : Wednesday, October 9, 2024 3:35:08 AM
Default Gateway . . . . . : 192.168.88.1
DHCP Server . . . . . : 192.168.88.1
DHCPv6 IAID . . . . . : 626794679
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-32-CA-37-00-93-37-DB-97-AF
DNS Servers . . . . . : 192.168.88.1
NetBIOS over Tcpip. . . . . : Enabled
```

Như hình ảnh bên cạnh, DNS cục bộ có địa chỉ IP là 192.168.88.1, có giá trị bằng giá trị của cột Destination IP trong các packet truy vấn, tức là truy vấn DNS đã được gửi đến máy chủ DNS cục bộ của em.

17. Kiểm tra tin nhắn truy vấn DNS. "Loại" (Type) của truy vấn DNS là gì? Tin nhắn truy vấn có chứa bất kỳ "câu trả lời" nào không?

```
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Destination: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Source: Intel_db:97:af (00:93:37:db:97:af)
Type: IPv4 (0x0800)
[Stream index: 0]
```

Trong ví dụ trên, có trường Type: Ipv4, tức là truy vấn tìm địa chỉ IP của một tên miền.

Trong các tin nhắn truy vấn DNS, ta sẽ không thấy bất kỳ "câu trả lời" nào, vì nó chỉ đang gửi yêu cầu tới máy chủ DNS để lấy thông tin. Thông thường, các "câu trả lời" chỉ xuất hiện trong gói tin phản hồi DNS (DNS response), không có trong gói truy vấn.

18. Kiểm tra tin nhắn phản hồi DNS. Các máy chủ tên (nameserver) của MIT mà tin nhắn phản hồi cung cấp là gì? Tin nhắn phản hồi này có cung cấp địa chỉ IP của các máy chủ tên của MIT không?

No.	Time	Source	Destination	Protocol	Length	Info
878	20:58:22.623840	192.168.88.1	192.168.88.159	DNS	234	Standard query response 0x0002 NS mit.edu NS usw2.akam.net NS ns1-173.akam.net NS ns1-37.akam.net NS use5.akam.net NS use2.akam.net NS asia1.akam.net NS eur5.akam.net NS asia2.akam.net

Trong phản hồi DNS này, chỉ có các tên của máy chủ (nameserver) được cung cấp mà không có địa chỉ IP kèm theo. Điều này có nghĩa là để lấy được địa chỉ IP của các máy chủ tên này, một truy vấn DNS tiếp theo (hoặc nhiều truy vấn khác) cần được gửi đến để lấy thông tin địa chỉ IP tương ứng.

19. Cung cấp một ảnh chụp màn hình.

Em đã cung cấp đầy đủ ở trên.

Bây giờ lặp lại thí nghiệm trước đó, nhưng thay vào đó, thực hiện lệnh:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

```
D:\Workspaces>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
Server:    Unknown
Address:   18.0.72.3

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out
```

No.	dns	Source	Destination	Protocol	Length	Info
131	21:07:15.398732	192.168.88.159	192.168.88.1	DNS	73	Standard query 0xa696 A bitsy.mit.edu
132	21:07:15.424892	192.168.88.1	192.168.88.159	DNS	73	Standard query 0xa696 A bitsy.mit.edu
133	21:07:15.426906	192.168.88.159	18.0.72.3	DNS	89	Standard query response 0xa696 A bitsy.mit.edu A 18.0.72.3
144	21:07:17.439366	192.168.88.159	18.0.72.3	DNS	82	Standard query 0x0003 PTR 3.72.0.18.in-addr.arpa
187	21:07:19.447810	192.168.88.159	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
204	21:07:21.456288	192.168.88.159	18.0.72.3	DNS	74	Standard query 0x0004 AAAA www.aiit.or.kr
225	21:07:23.469484	192.168.88.159	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
286	21:07:27.117199	192.168.88.159	192.168.88.1	DNS	87	Standard query 0x019d A tt-profile-wpa.chat.zalo.me
288	21:07:27.129954	192.168.88.1	192.168.88.159	DNS	135	Standard query response 0x019d A tt-profile-wpa.chat.zalo.me A 49.213.95.182 A 49.213.95.137 A 49.213.95.187
314	21:07:27.180748	192.168.88.159	192.168.88.1	DNS	87	Standard query 0xe7fd A tt-sticker-wpa.chat.zalo.me
315	21:07:27.186883	192.168.88.1	192.168.88.159	DNS	103	Standard query response 0xe7fd A tt-sticker-wpa.chat.zalo.me A 49.213.95.122
1063	21:07:50.702595	192.168.88.159	192.168.88.1	DNS	98	Standard query 0xbbad A securetoken.googleapis.com
1067	21:07:50.703739	192.168.88.159	192.168.88.1	DNS	98	Standard query 0xd9aa HTTPS securetoken.googleapis.com
1072	21:07:50.721150	192.168.88.159	192.168.88.1	DNS	157	Standard query response 0xd9aa HTTPS securetoken.googleapis.com SOA ns1.google.com
1074	21:07:50.722401	192.168.88.1	192.168.88.159	DNS	356	Standard query response 0xbbad A securetoken.googleapis.com A 142.250.76.10 A 142.250.76.234 A 142.250.197.10 A 142.250.197.42 A 142.250.197.74 A 142.250.197.100 A 142.250.197.101 A 142.250.197.102 A 142.250.197.103 A 142.250.197.104 A 142.250.197.105 A 142.250.197.106 A 142.250.197.107 A 142.250.197.108 A 142.250.197.109 A 142.250.197.110 A 142.250.197.111 A 142.250.197.112 A 142.250.197.113 A 142.250.197.114 A 142.250.197.115 A 142.250.197.116 A 142.250.197.117 A 142.250.197.118 A 142.250.197.119 A 142.250.197.120 A 142.250.197.121 A 142.250.197.122 A 142.250.197.123 A 142.250.197.124 A 142.250.197.125 A 142.250.197.126 A 142.250.197.127 A 142.250.197.128 A 142.250.197.129 A 142.250.197.130 A 142.250.197.131 A 142.250.197.132 A 142.250.197.133 A 142.250.197.134 A 142.250.197.135 A 142.250.197.136 A 142.250.197.137 A 142.250.197.138 A 142.250.197.139 A 142.250.197.140 A 142.250.197.141 A 142.250.197.142 A 142.250.197.143 A 142.250.197.144 A 142.250.197.145 A 142.250.197.146 A 142.250.197.147 A 142.250.197.148 A 142.250.197.149 A 142.250.197.150 A 142.250.197.151 A 142.250.197.152 A 142.250.197.153 A 142.250.197.154 A 142.250.197.155 A 142.250.197.156 A 142.250.197.157 A 142.250.197.158 A 142.250.197.159 A 142.250.197.160 A 142.250.197.161 A 142.250.197.162 A 142.250.197.163 A 142.250.197.164 A 142.250.197.165 A 142.250.197.166 A 142.250.197.167 A 142.250.197.168 A 142.250.197.169 A 142.250.197.170 A 142.250.197.171 A 142.250.197.172 A 142.250.197.173 A 142.250.197.174 A 142.250.197.175 A 142.250.197.176 A 142.250.197.177 A 142.250.197.178 A 142.250.197.179 A 142.250.197.180 A 142.250.197.181 A 142.250.197.182 A 142.250.197.183 A 142.250.197.184 A 142.250.197.185 A 142.250.197.186 A 142.250.197.187 A 142.250.197.188 A 142.250.197.189 A 142.250.197.190 A 142.250.197.191 A 142.250.197.192 A 142.250.197.193 A 142.250.197.194 A 142.250.197.195 A 142.250.197.196 A 142.250.197.197 A 142.250.197.198 A 142.250.197.199 A 142.250.197.200 A 142.250.197.201 A 142.250.197.202 A 142.250.197.203 A 142.250.197.204 A 142.250.197.205 A 142.250.197.206 A 142.250.197.207 A 142.250.197.208 A 142.250.197.209 A 142.250.197.210 A 142.250.197.211 A 142.250.197.212 A 142.250.197.213 A 142.250.197.214 A 142.250.197.215 A 142.250.197.216 A 142.250.197.217 A 142.250.197.218 A 142.250.197.219 A 142.250.197.220 A 142.250.197.221 A 142.250.197.222 A 142.250.197.223 A 142.250.197.224 A 142.250.197.225 A 142.250.197.226 A 142.250.197.227 A 142.250.197.228 A 142.250.197.229 A 142.250.197.230 A 142.250.197.231 A 142.250.197.232 A 142.250.197.233 A 142.250.197.234 A 142.250.197.235 A 142.250.197.236 A 142.250.197.237 A 142.250.197.238 A 142.250.197.239 A 142.250.197.240 A 142.250.197.241 A 142.250.197.242 A 142.250.197.243 A 142.250.197.244 A 142.250.197.245 A 142.250.197.246 A 142.250.197.247 A 142.250.197.248 A 142.250.197.249 A 142.250.197.250 A 142.250.197.251 A 142.250.197.252 A 142.250.197.253 A 142.250.197.254 A 142.250.197.255 A 142.250.197.256 A 142.250.197.257 A 142.250.197.258 A 142.250.197.259 A 142.250.197.260 A 142.250.197.261 A 142.250.197.262 A 142.250.197.263 A 142.250.197.264 A 142.250.197.265 A 142.250.197.266 A 142.250.197.267 A 142.250.197.268 A 142.250.197.269 A 142.250.197.270 A 142.250.197.271 A 142.250.197.272 A 142.250.197.273 A 142.250.197.274 A 142.250.197.275 A 142.250.197.276 A 142.250.197.277 A 142.250.197.278 A 142.250.197.279 A 142.250.197.280 A 142.250.197.281 A 142.250.197.282 A 142.250.197.283 A 142.250.197.284 A 142.250.197.285 A 142.250.197.286 A 142.250.197.287 A 142.250.197.288 A 142.250.197.289 A 142.250.197.290 A 142.250.197.291 A 142.250.197.292 A 142.250.197.293 A 142.250.197.294 A 142.250.197.295 A 142.250.197.296 A 142.250.197.297 A 142.250.197.298 A 142.250.197.299 A 142.250.197.300 A 142.250.197.301 A 142.250.197.302 A 142.250.197.303 A 142.250.197.304 A 142.250.197.305 A 142.250.197.306 A 142.250.197.307 A 142.250.197.308 A 142.250.197.309 A 142.250.197.310 A 142.250.197.311 A 142.250.197.312 A 142.250.197.313 A 142.250.197.314 A 142.250.197.315 A 142.250.197.316 A 142.250.197.317 A 142.250.197.318 A 142.250.197.319 A 142.250.197.320 A 142.250.197.321 A 142.250.197.322 A 142.250.197.323 A 142.250.197.324 A 142.250.197.325 A 142.250.197.326 A 142.250.197.327 A 142.250.197.328 A 142.250.197.329 A 142.250.197.330 A 142.250.197.331 A 142.250.197.332 A 142.250.197.333 A 142.250.197.334 A 142.250.197.335 A 142.250.197.336 A 142.250.197.337 A 142.250.197.338 A 142.250.197.339 A 142.250.197.340 A 142.250.197.341 A 142.250.197.342 A 142.250.197.343 A 142.250.197.344 A 142.250.197.345 A 142.250.197.346 A 142.250.197.347 A 142.250.197.348 A 142.250.197.349 A 142.250.197.350 A 142.250.197.351 A 142.250.197.352 A 142.250.197.353 A 142.250.197.354 A 142.250.197.355 A 142.250.197.356 A 142.250.197.357 A 142.250.197.358 A 142.250.197.359 A 142.250.197.360 A 142.250.197.361 A 142.250.197.362 A 142.250.197.363 A 142.250.197.364 A 142.250.197.365 A 142.250.197.366 A 142.250.197.367 A 142.250.197.368 A 142.250.197.369 A 142.250.197.370 A 142.250.197.371 A 142.250.197.372 A 142.250.197.373 A 142.250.197.374 A 142.250.197.375 A 142.250.197.376 A 142.250.197.377 A 142.250.197.378 A 142.250.197.379 A 142.250.197.380 A 142.250.197.381 A 142.250.197.382 A 142.250.197.383 A 142.250.197.384 A 142.250.197.385 A 142.250.197.386 A 142.250.197.387 A 142.250.197.388 A 142.250.197.389 A 142.250.197.390 A 142.250.197.391 A 142.250.197.392 A 142.250.197.393 A 142.250.197.394 A 142.250.197.395 A 142.250.197.396 A 142.250.197.397 A 142.250.197.398 A 142.250.197.399 A 142.250.197.400 A 142.250.197.401 A 142.250.197.402 A 142.250.197.403 A 142.250.197.404 A 142.250.197.405 A 142.250.197.406 A 142.250.197.407 A 142.250.197.408 A 142.250.197.409 A 142.250.197.410 A 142.250.197.411 A 142.250.197.412 A 142.250.197.413 A 142.250.197.414 A 142.250.197.415 A 142.250.197.416 A 142.250.197.417 A 142.250.197.418 A 142.250.197.419 A 142.250.197.420 A 142.250.197.421 A 142.250.197.422 A 142.250.197.423 A 142.250.197.424 A 142.250.197.425 A 142.250.197.426 A 142.250.197.427 A 142.250.197.428 A 142.250.197.429 A 142.250.197.430 A 142.250.197.431 A 142.250.197.432 A 142.250.197.433 A 142.250.197.434 A 142.250.197.435 A 142.250.197.436 A 142.250.197.437 A 142.250.197.438 A 142.250.197.439 A 142.250.197.440 A 142.250.197.441 A 142.250.197.442 A 142.250.197.443 A 142.250.197.444 A 142.250.197.445 A 142.250.197.446 A 142.250.197.447 A 142.250.197.448 A 142.250.197.449 A 142.250.197.450 A 142.250.197.451 A 142.250.197.452 A 142.250.197.453 A 142.250.197.454 A 142.250.197.455 A 142.250.197.456 A 142.250.197.457 A 142.250.197.458 A 142.250.197.459 A 142.250.197.460 A 142.250.197.461 A 142.250.197.462 A 142.250.197.463 A 142.250.197.464 A 142.250.197.465 A 142.250.197.466 A 142.250.197.467 A 142.250.197.468 A 142.250.197.469 A 142.250.197.470 A 142.250.197.471 A 142.250.197.472 A 142.250.197.473 A 142.250.197.474 A 142.250.197.475 A 142.250.197.476 A 142.250.197.477 A 142.250.197.478 A 142.250.197.479 A 142.250.197.480 A 142.250.197.481 A 142.250.197.482 A 142.250.197.483 A 142.250.197.484 A 142.250.197.485 A 142.250.197.486 A 142.250.197.487 A 142.250.197.488 A 142.250.197.489 A 142.250.197.490 A 142.250.197.491 A 142.250.197.492 A 142.250.197.493 A 142.250.197.494 A 142.250.197.495 A 142.250.197.496 A 142.250.197.497 A 142.250.197.498 A 142.250.197.499 A 142.250.197.500 A 142.250.197.501 A 142.250.197.502 A 142.250.197.503 A 142.250.197.504 A 142.250.197.505 A 142.250.197.506 A 142.250.197.507 A 142.250.197.508 A 142.250.197.509 A 142.250.197.510 A 142.250.197.511 A 142.250.197.512 A 142.250.197.513 A 142.250.197.514 A 142.250.197.515 A 142.250.197.516 A 142.250.197.517 A 142.250.197.518 A 142.250.197.519 A 142.250.197.520 A 142.250.197.521 A 142.250.197.522 A 142.250.197.523 A 142.250.197.524 A 142.250.197.525 A 142.250.197.526 A 142.250.197.527 A 142.250.197.528 A 142.250.197.529 A 142.250.197.530 A 142.250.197.531 A 142.250.197.532 A 142.250.197.533 A 142.250.197.534 A 142.250.197.535 A 142.250.197.536 A 142.250.197.537 A 142.250.197.538 A 142.250.197.539 A 142.250.197.540 A 142.250.197.541 A 142.250.197.542 A 142.250.197.543 A 142.250.197.544 A 142.250.197.545 A 142.250.197.546 A 142.250.197.547 A 142.250.197.548 A 142.250.197.549 A 142.250.197.550 A 142.250.197.551 A 142.250.197.552 A 142.250.197.553 A 142.250.197.554 A 142.250.197.555 A 142.250.197.556 A 142.250.197.557 A 142.250.197.558 A 142.250.197.559 A 142.250.197.560 A 142.250.197.561 A 142.250.197.562 A 142.250.197.563 A 142.250.197.564 A 142.250.197.565 A 142.250.197.566 A 142.250.197.567 A 142.250.197.568 A 142.250.197.569 A 142.250.197.570 A 142.250.197.571 A 142.250.197.572 A 142.250.197.573 A 142.250.197.574 A 142.250.197.575 A 142.250.197.576 A 142.250.197.577 A 142.250.197.578 A 142.250.197.579 A 142.250.197.580 A 142.250.197.581 A 142.250.197.582 A 142.250.197.583 A 142.250.197.584 A 142.250.197.585 A 142.250.197.586 A 142.250.197.587 A 142.250.197.588 A 142.250.197.589 A 142.250.197.590 A 142.250.197.591 A 142.250.197.592 A 142.250.197.593 A 142.250.197.594 A 142.250.197.595 A 142.250.197.596 A 142.250.197.597 A 142.250.197.598 A 142.250.197.599 A 142.250.197.600 A 142.250.197.601 A 142.250.197.602 A 142.250.197.603 A 142.250.197.604 A 142.250.197.605 A 142.250.197.606 A 142.250.197.607 A 142.250.197.608 A 142.250.197.609 A 142.250.197.610 A 142.250.197.611 A 142.250.197.612 A 142.250.197.613 A 142.250.197.614 A 142.250.197.615 A 142.250.197.616 A 142.250.197.617 A 142.250.197.618 A 142.250.197.619 A 142.250.197.620 A 142.250.197.621 A 142.250.197.622 A 142.250.197.623 A 142.250.197.624 A 142.250.197.625 A 142.250.197.626 A 142.250.197.627 A 142.250.197.628 A 142.250.197.629 A 142.250.197.630 A 142.250.197.631 A 142.250.197.632 A 142.250.197.633 A 142.250.197.634 A 142.250.197.635 A 142.250.197.636 A 142.250.197.637 A 142.250.197.638 A 142.250.197.639 A 142.250.197.640 A 142.250.197.641 A 142.250.197.642 A 142.250.197.643 A 142.250.197.644 A 142.250.197.645 A 142.250.197.646 A 142.250.197.647 A 142.250.197.648 A 142.250.197.649 A 142.250.197.650 A 142.250.197.651 A 142.250.197.652 A 142.250.197.653 A 142.250.197.654 A 142.250.197.655 A 142.250.197.656 A 142.250.197.657 A 142.250.197.658 A 142.250.197.659 A 142.250.197.660 A 142.250.197.661 A 142.250.197.662 A 142.250.197.663 A 142.250.197.664 A 142.250.197.665 A 142.250.197.666 A 142.250.197.667 A 142.250.197.668 A 142.250.197.669 A 142.250.197.670 A 142.250.197.671 A 142.250.197.672 A 142.250.197.673 A 142.250.197.674 A 142.250.197.675 A 142.250.197.676 A 142.250.197.677 A 142.250.197.678 A 142.250.197.679 A 142.250.197.680 A 142.250.197.681 A 142.250.197.682 A 142.250.197.683 A 142.250.197.684 A 142.250.197.685 A 142.250.197.686 A 142.250.197.687 A 142.250.197.688 A 142.250.197.689 A 142.

Trả lời các câu hỏi sau

20. Tin nhắn truy vấn DNS được gửi đến địa chỉ IP nào? Đây có phải là địa chỉ IP của máy chủ DNS cục bộ mặc định của bạn không? Nếu không, địa chỉ IP này tương ứng với gì?

No.	Time	Source	Destination	Protocol	Length	Info
131	21:07:15.398732	192.168.88.159	192.168.88.1	DNS	73	Standard query 0xa696 A bitsy.mit.edu

```
Wireless LAN adapter Wi-Fi 2:
Connection-specific DNS Suffix . : lan
Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . : 08-93-37-DB-97-AF
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%21(Preferred)
IPv4 Address. . . . . : 192.168.88.159(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, October 6, 2024 11:48:46 AM
Lease Expires . . . . . : Wednesday, October 9, 2024 3:35:08 AM
Default Gateway . . . . . : 192.168.88.1
DHCP Server . . . . . : 192.168.88.1
DHCPv6 IAID . . . . . : 620794679
DHCPv6 Client DUID. . . . . : 08-01-00-01-2E-32-CA-37-00-93-37-DB-97-AF
DNS Servers . . . . . : 192.168.88.1
NetBIOS over Tcpip. . . . . : Enabled
```

Như hình ảnh bên cạnh, DNS cục bộ có địa chỉ IP là 192.168.88.1, có giá trị bằng giá trị của cột Destination IP trong các packet truy vấn, tức là truy vấn DNS đã được gửi đến máy chủ DNS cục bộ của em.

21. Kiểm tra tin nhắn truy vấn DNS. "Loại" (Type) của truy vấn DNS là gì? Tin nhắn truy vấn có chứa bất kỳ "câu trả lời" nào không?

```
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Destination: VietnamPostA_f2:d0:ce (cc:71:90:f2:d0:ce)
Source: Intel db:97:af (00:93:37:db:97:af)
Type: IPv4 (0x0800)
[Stream index: 0]
```

Trong ví dụ trên, có trường Type: Ipv4, tức là truy vấn tìm địa chỉ IP của một tên miền. Trong các tin nhắn truy vấn DNS, ta sẽ không thấy bất kỳ "câu trả lời" nào, vì nó chỉ đang gửi yêu cầu tới máy chủ DNS để lấy thông tin. Thông thường, các "câu trả lời" chỉ xuất hiện trong gói tin phản hồi DNS (DNS response), không có trong gói truy vấn.

22. Kiểm tra tin nhắn phản hồi DNS. Có bao nhiêu "câu trả lời" được cung cấp? Mỗi câu trả lời chứa gì?

No.	Time	Source	Destination	Protocol	Length	Info
132	21:07:15.424892	192.168.88.1	192.168.88.159	DNS	89	Standard query response 0xa696 A bitsy.mit.edu
A	18.0.72.3					


```
Domain Name System (response)
Transaction ID: 0xa696
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
  bitsy.mit.edu: type A, class IN
    Name: bitsy.mit.edu
    [Name Length: 13]
    [Label Count: 3]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
Answers
[Request In: 130]
[Time: 0.063154000 seconds]
```

Trong ví dụ này, em chọn gói tin phản hồi 6465, Answer RRs: 1 cho biết có 1 "câu trả lời" (RR - Resource Records) trong phản hồi này.

23. Cung cấp một ảnh chụp màn hình.

Em đã cung cấp đầy đủ ở trên.