

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 THỰC HÀNH - CO3094

Báo cáo:

Lab2b

Giảng viên hướng dẫn: Vũ Thành Tài

Sinh viên: Lê Đức Cường

Thành phố Hồ Chí Minh, tháng 3 năm 2025

1 Question 1

Run nslookup to obtain the IP address of a Web server in Asia. What is the IP address of that server?

I used nslookup on hcmut.edu.vn

```
C:\Users\Admin>nslookup hcmut.edu.vn
Server: XiaoQiang
Address: 192.168.31.1

Non-authoritative answer:
Name: hcmut.edu.vn
Address: 113.161.119.157

C:\Users\Admin>
```

2 Question 2

Run nslookup to determine the authoritative DNS servers for a university in Europe.

```
C:\Users\Admin>nslookup -type=NS www.cam.ac.uk
Server: XiaoQiang
Address: 192.168.31.1

cam.ac.uk
    primary name server = primary.dns.cam.ac.uk
    responsible mail addr = hostmaster.cam.ac.uk
    serial = 1741945497
    refresh = 1800 (30 mins)
    retry = 900 (15 mins)
    expire = 604800 (7 days)
    default TTL = 3600 (1 hour)
```

3 Question 3

Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

The IP address for the DNS server if queried for the Yahoo! mail server is 180.222.116.12

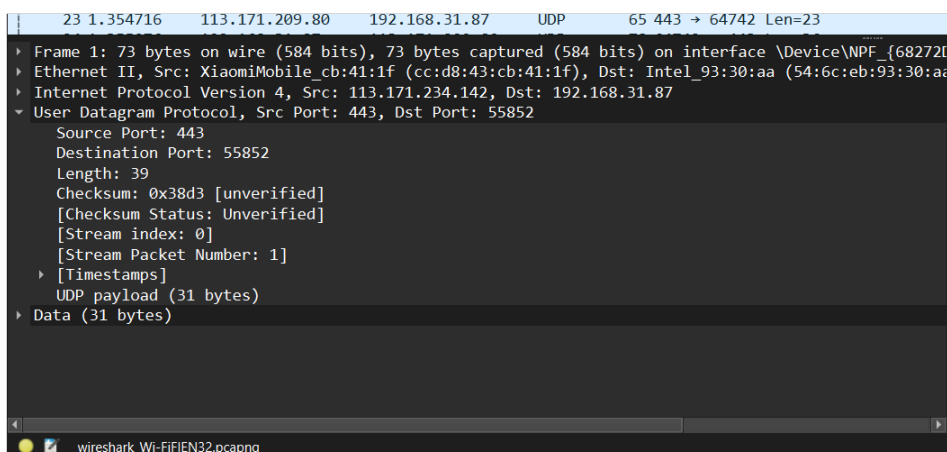
```
C:\Users\Admin>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  180.222.116.12

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
```

4 Question 4

Locate the DNS query and response messages. Are then sent over UDP or TCP?

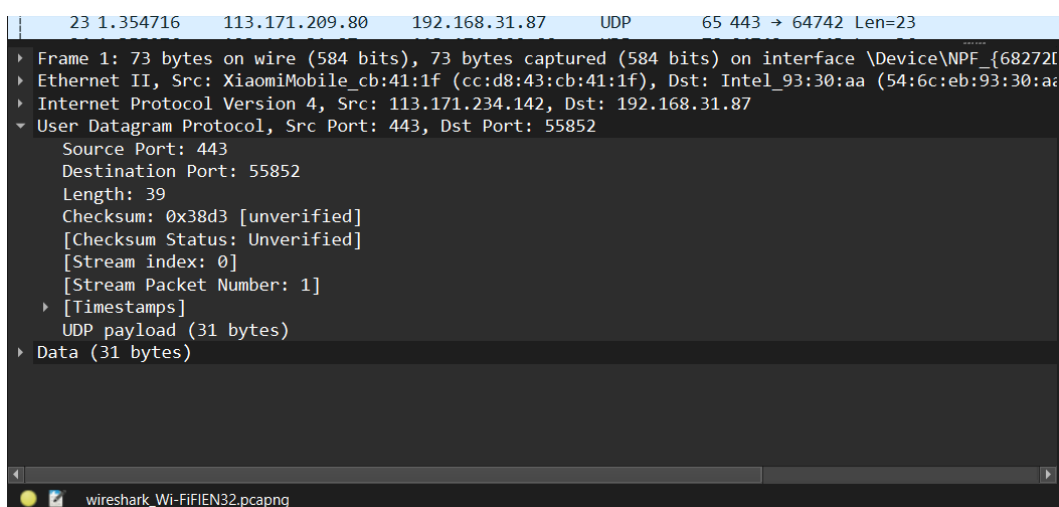
UDP



5 Question 5

What is the destination port for the DNS query message? What is the source port of DNS response message?

- The destination port is 55852
- The source port is 443



6 Question 6

To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query was sent to IP address 192.168.31.1 and it is the same IP address as that of my local DNS server.

No.	Time	Source	Destination	Protocol	Length	Info
843	8.476296	192.168.31.87	104.16.45.99	QUIC	1292	Protected Payload (KP0), DCID=01f3fd3bc1d2be67b9f1b83bd0d2889bd6a988c6
844	8.476500	192.168.31.87	104.16.45.99	QUIC	161	Protected Payload (KP0), DCID=01f3fd3bc1d2be67b9f1b83bd0d2889bd6a988c6
845	8.481862	192.168.31.87	104.16.45.99	TCP	54	59500 → 443 [ACK] Seq=172 Ack=262 Win=513 Len=0
846	8.503904	20.189.173.12	192.168.31.87	TCP	54	443 → 59334 [ACK] Seq=134 Ack=1566 Win=16385 Len=0
847	8.545976	104.16.45.99	192.168.31.87	QUIC	66	Protected Payload (KP0)
848	8.577506	192.168.31.87	192.168.31.1	DNS	72	Standard query 0xe948 A www.ietf.org
849	8.579006	192.168.31.1	192.168.31.87	DNS	104	Standard query response 0xe948 A www.ietf.org A 104.16.45.99 A 104.16.44.99
850	8.579478	192.168.31.87	104.16.45.99	QUIC	933	Protected Payload (KP0), DCID=01f3fd3bc1d2be67b9f1b83bd0d2889bd6a988c6
851	8.617271	104.16.45.99	192.168.31.87	QUIC	66	Protected Payload (KP0)

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
Physical Address. . . . . : 54-6C-EB-93-30-AA
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b3fa:f577:e55e:5f9b%11(Preferred)
IPv4 Address. . . . . : 192.168.31.87(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 14 March 2025 12:48:48
Lease Expires . . . . . : 15 March 2025 08:08:59
Default Gateway . . . . . : 192.168.31.1
DHCP Server . . . . . : 192.168.31.1
DHCPv6 IAID . . . . . : 122973419
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-FE-23-0B-0C-37-96-6F-D4-00
DNS Servers . . . . . : 192.168.31.1
NetBIOS over Tcpip. . . . . : Enabled
```

7 Question 7

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The query message was a type “A” query, but the message did not contain any “answers.”

```
Domain Name System (query)
Transaction ID: 0xe948
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  www.ietf.org: type A, class IN
```

8 Question 8

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

The response message contained one answer to the query which was the sites address 104.16.45.99.

```
▶ Internet Protocol Version 4, Src: 192.168.31.1, Dst: 192.168.31.87
▶ User Datagram Protocol, Src Port: 53, Dst Port: 52046
▼ Domain Name System (response)
  Transaction ID: 0xa621
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▼ www.ietf.org: type A, class IN, addr 104.16.45.99
      Name: www.ietf.org
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 4
      Address: 104.16.45.99
```

9 Question 9

Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The destination of the SYN packet is 104.16.45.99, the same address that was provided in the DNS response message as the type “A” address of the webpage.

10 Question 10

This web page contains images. Before retrieving each image, does your host issue new DNS queries?

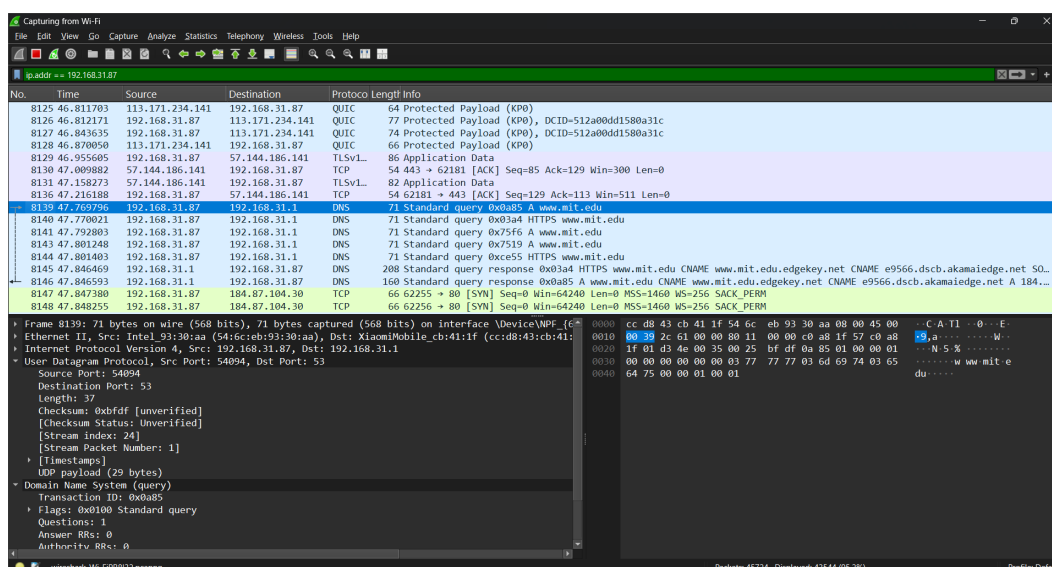
No, the images are all loaded from www.ietf.org, so no additional DNS queries are necessary, the host uses a cached address.



11 Question 11

What is the destination port for the DNS query message? What is the source port of DNS response message?

- Destination Port: 53
- Source Port: 54094



12 Question 12

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

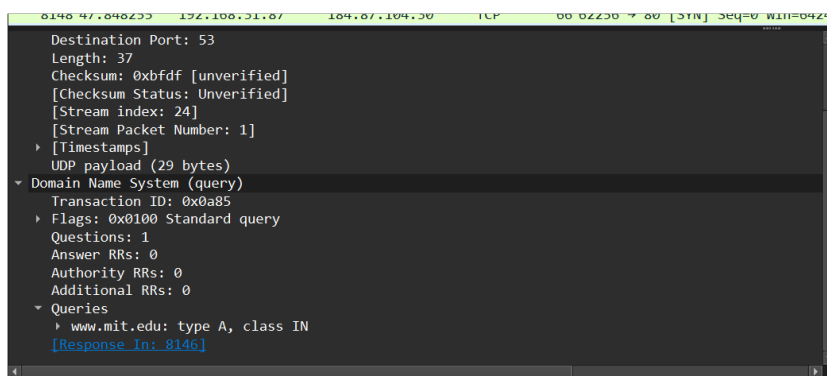
The DNS query message is sent to IP address 192.168.31.1, the same address as my default local DNS server.

8139	47.769796	192.168.31.87	192.168.31.1	DNS	71	Standard query 0x0a85 A www.mit.edu
8140	47.770021	192.168.31.87	192.168.31.1	DNS	71	Standard query 0x03a4 HTTPS www.mit.edu
8141	47.792803	192.168.31.87	192.168.31.1	DNS	71	Standard query 0x75f6 A www.mit.edu
8143	47.801248	192.168.31.87	192.168.31.1	DNS	71	Standard query 0x7519 A www.mit.edu
8144	47.801403	192.168.31.87	192.168.31.1	DNS	71	Standard query 0xce55 HTTPS www.mit.edu
8145	47.846469	192.168.31.1	192.168.31.87	DNS	208	Standard query response 0x03a4 HTTPS www.mit.edu CNAME www.mit.edu.edgekey.net
8146	47.846593	192.168.31.1	192.168.31.87	DNS	160	Standard query response 0x0a85 A www.mit.edu CNAME www.mit.edu.edgekey.net

13 Question 13

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

The DNS query message is a type “A” query, containing only one question and not containing any answers.

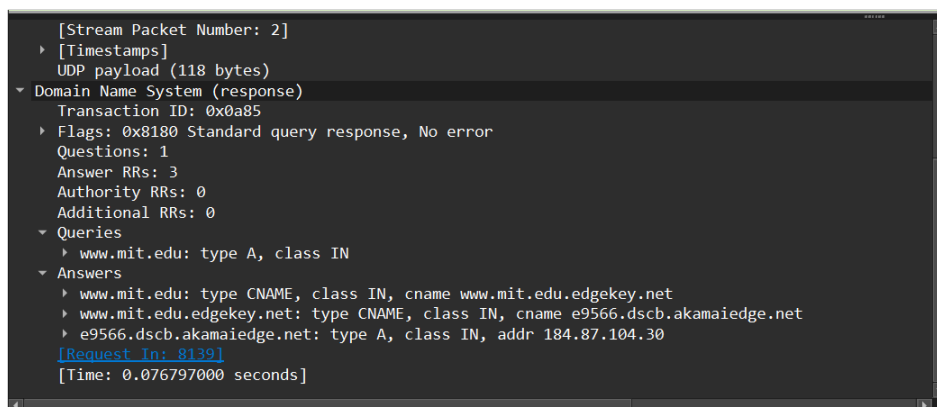


```
0148 47.040233 132.166.21.87 184.87.104.30 TCP 60 02230 → 80 [STN] Seq=0 Win=04240
Destination Port: 53
Length: 37
Checksum: 0xbfdf [unverified]
[Checksum Status: Unverified]
[Stream index: 24]
[Stream Packet Number: 1]
[Timestamps]
  UDP payload (29 bytes)
    Domain Name System (query)
      Transaction ID: 0x0a85
      Flags: 0x0100 Standard query
      Questions: 1
      Answer RRs: 0
      Authority RRs: 0
      Additional RRs: 0
      Queries
        www.mit.edu: type A, class IN
        [Response in: 8146]
```

14 Question 14

Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?

The response message contains one answer to the aforementioned query which is the type “A” address of 184.87.104.30. It also contained information on 3 authoritative nameservers and 3 additional records.



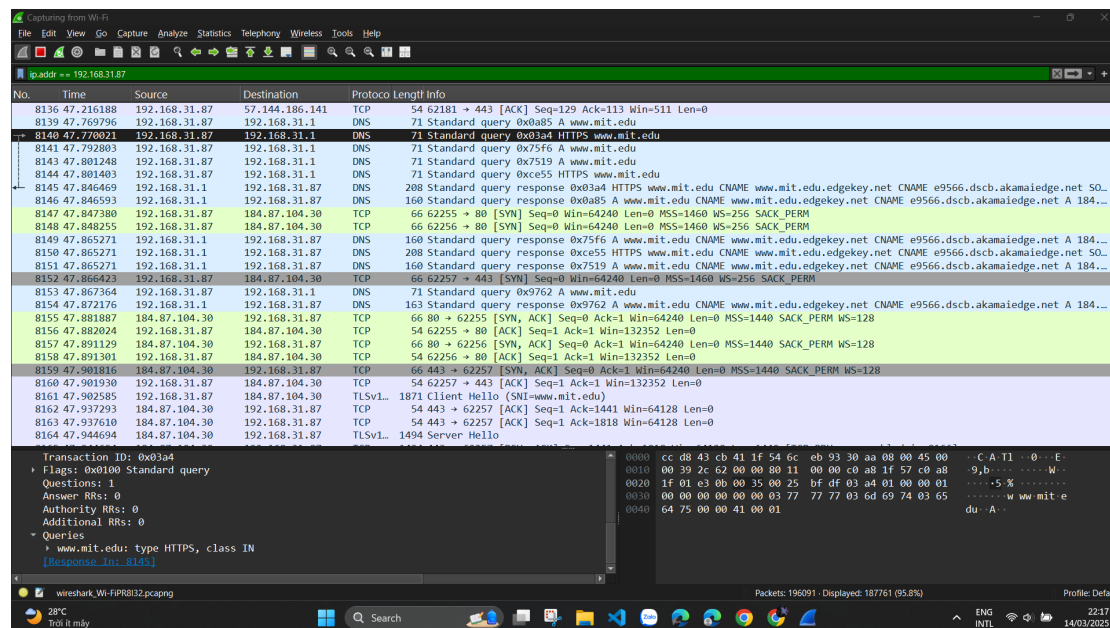
```
[Stream Packet Number: 2]
[Timestamps]
  UDP payload (118 bytes)
    Domain Name System (response)
      Transaction ID: 0x0a85
      Flags: 0x8100 Standard query response, No error
      Questions: 1
      Answer RRs: 3
      Authority RRs: 0
      Additional RRs: 0
      Queries
        www.mit.edu: type A, class IN
      Answers
        www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type A, class IN, addr 184.87.104.30
        [Request in: 8139]
      [Time: 0.076797000 seconds]
```




774 2.612103	40.119.213.159	192.168.31.87	TLSv1...	78 Application Data
777 2.819631	192.168.31.87	192.168.31.1	DNS	67 Standard query 0x9086 A mit.edu
778 2.880739	192.168.31.1	192.168.31.87	DNS	83 Standard query response 0x9086 A mit.edu A 23.59.9.193
779 2.884594	192.168.31.87	23.59.9.193	DNS	84 Standard query 0x0001 PTR 193.9.59.23.in-addr.arpa

15 Question 15

Provide a screenshot.



16 Question 16

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

The query is sent to 192.168.31.1, the same IP address as that of my default local DNS server.

17 Question 17

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?



```
Transaction ID: 0x0002
  Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    www.mit.edu: type NS, class IN
    [Response In: 1148]
```

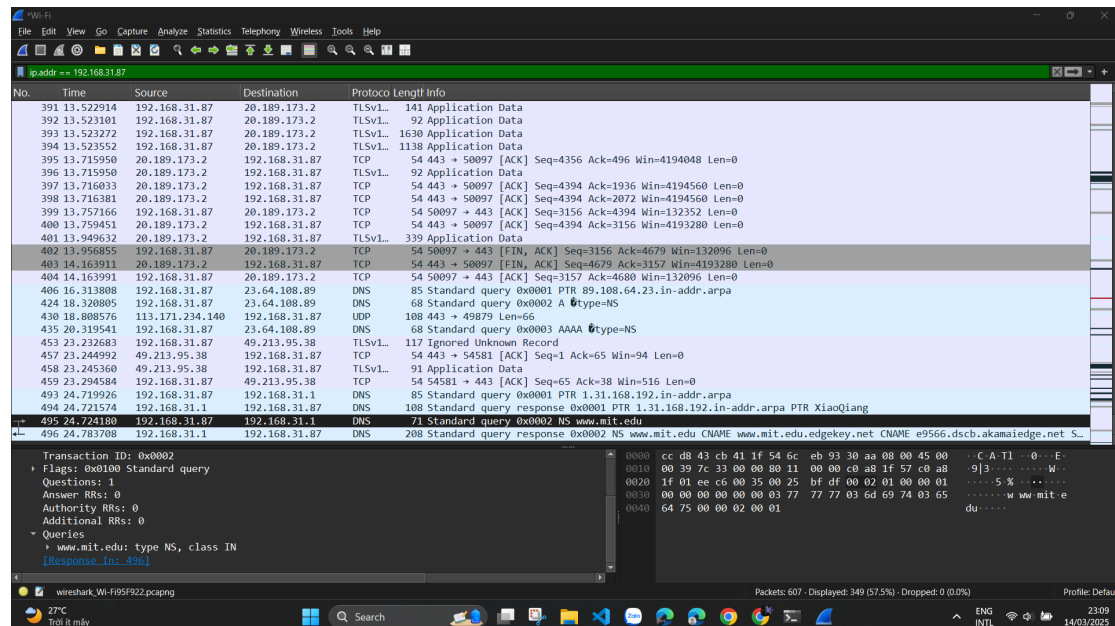
18 Question 18

Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?

Contain name, type, class, TTL, Data length, CNAME.

19 Question 19

Provide a screenshot.



20 Question 20

To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to? This DNS query message is sent to 192.168.31.1 which is the IP address of the MIT DNS response sender.

Time	Source IP	Destination IP	Protocol	Details
36 5.311177	192.168.31.87	192.168.31.1	DNS	73 Standard query 0x6e44 A bitsy.mit.edu
37 5.370925	192.168.31.87	192.168.31.1	DNS	73 Standard query 0x6e44 A bitsy.mit.edu
38 5.372764	192.168.31.1	192.168.31.87	DNS	89 Standard query response 0x6e44 A bitsy.mit.edu A 18.0.72.3
39 5.372830	192.168.31.1	192.168.31.87	DNS	89 Standard query response 0x6e44 A bitsy.mit.edu A 18.0.72.3

21 Question 21

Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?

This DNS query is a type “A” query. The message does not contain any answers.

```
Transaction ID: 0x6e44
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    bitsy.mit.edu: type A, class IN
    [Response in: 38]
```

22 Question 22

Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?

It only provided one “answer” containing the servers IP address, however, the server also returned a flag that stated that it could complete a recursive query.



23 Question 23

Provide a screenshot.

