

# Computer Networks

*LAB 3b*

Author:

Tran Dinh Dang Khoa  
2211649

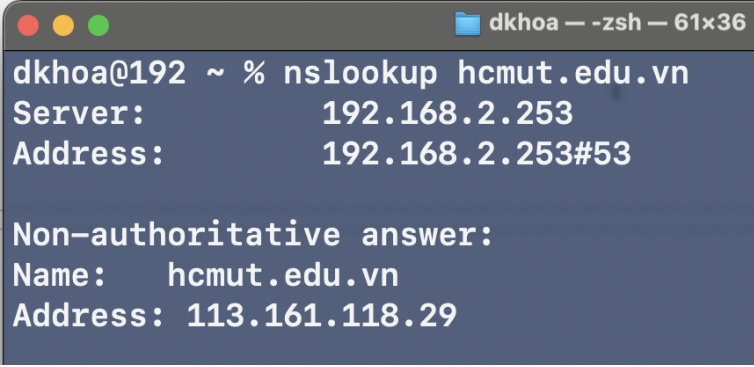
Date: October 12, 2024

## Contents

1	nslookup	2
2	Tracing DNS with Wireshark	4

## 1 nslookup

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

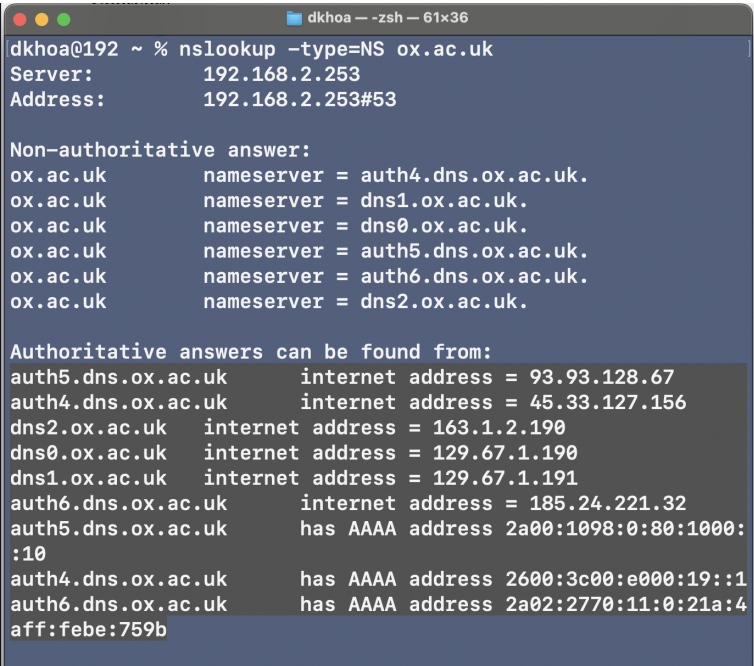


```
dkhoa@192 ~ % nslookup hcmut.edu.vn
Server:          192.168.2.253
Address:         192.168.2.253#53

Non-authoritative answer:
Name:   hcmut.edu.vn
Address: 113.161.118.29
```

hcmut.edu.vn is a Vietnamese web server. The IP address is 113.161.118.29

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



```
dkhoa@192 ~ % nslookup -type=NS ox.ac.uk
Server:          192.168.2.253
Address:         192.168.2.253#53

Non-authoritative answer:
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.

Authoritative answers can be found from:
auth5.dns.ox.ac.uk    internet address = 93.93.128.67
auth4.dns.ox.ac.uk    internet address = 45.33.127.156
dns2.ox.ac.uk         internet address = 163.1.2.190
dns0.ox.ac.uk         internet address = 129.67.1.190
dns1.ox.ac.uk         internet address = 129.67.1.191
auth6.dns.ox.ac.uk    internet address = 185.24.221.32
auth5.dns.ox.ac.uk    has AAAA address 2a00:1098:0:80:1000:
:10
auth4.dns.ox.ac.uk    has AAAA address 2600:3c00:e000:19::1
auth6.dns.ox.ac.uk    has AAAA address 2a02:2770:11:0:21a:4
aff:febe:759b
```

ox.ac.uk is the web server of Oxford University

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?

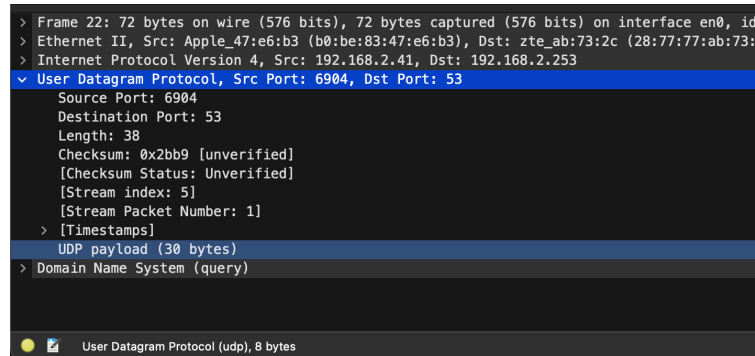
```
dkhoa@192 ~ % nslookup -type=MX yahoo.com dns1.ox.ac.uk
Server:      dns1.ox.ac.uk
Address:     129.67.1.191#53

** server can't find yahoo.com: REFUSED
```

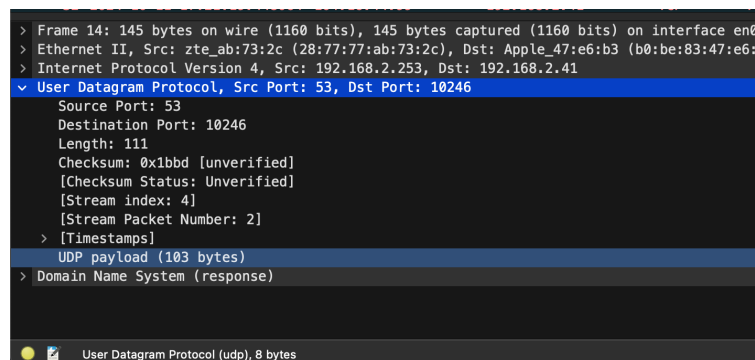
The server could not find yahoo.com

## 2 Tracing DNS with Wireshark

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



This is the DNS query message, it was sent over UDP



This is the DNS query response message, it's also sent over UDP

5. What is the destination port for the DNS query message? What is the source port of DNS response message?
- The destination port for the DNS query message: 53
  - The source port of the DNS response message: 53
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 message was sent to this IP address: 192.168.2.253

```
dkhoa@192 ~ % cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 192.168.2.253
dkhoa@192 ~ %
```

My local DNS server

- They are the same!

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

```
> Frame 22: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id
> Ethernet II, Src: Apple_47:e6:b3 (b0:be:83:47:e6:b3), Dst: zte_ab:73:2c (28:77:77:ab:73:
> Internet Protocol Version 4, Src: 192.168.2.41, Dst: 192.168.2.253
> User Datagram Protocol, Src Port: 6904, Dst Port: 53
  Domain Name System (query)
    Transaction ID: 0x1000
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
      > www.ietf.org: type A, class IN
      [Response In: 24]
```

DNS query type: type A. There was no “answer” in the query

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

```

> Frame 14: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface en0
> Ethernet II, Src: zte_ab:73:2c (28:77:77:ab:73:2c), Dst: Apple_47:e6:b3 (b0:be:83:47:e6:b3)
> Internet Protocol Version 4, Src: 192.168.2.253, Dst: 192.168.2.41
> User Datagram Protocol, Src Port: 53, Dst Port: 10246
< Domain Name System (response)
  Transaction ID: 0x1f16
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  < Queries
    > www.ietf.org: type HTTPS, class IN
  < Answers
    > www.ietf.org: type HTTPS, class IN
      Name: www.ietf.org
      Type: HTTPS (65) (HTTPS Specific Service Endpoints)
      Class: IN (0x0001)
      Time to live: 300 (5 minutes)
      Data length: 61
      SvcPriority: 1
      TargetName: <Root>
      > SvcParam: alpn=h3,h2
      > SvcParam: ipv4hint=104.16.44.99,104.16.45.99
      > SvcParam: ipv6hint=2606:4700::6810:2c63,2606:4700::6810:2d63
      [Request In: 11]
      [Time: 0.042296000 seconds]
  <
  Text item (text), 73 bytes

```

There is one answer in the response, it contains the web server information

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?

```

13 2024-10-11 17:21:19.196823 192.168.2.41 104.16.45.99 TCP 78 54464 -> 80 [SYN] Seq=0 Win
> Frame 13: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en0, id 0000 28 77 77 ab 73 2c b6
> Ethernet II, Src: Apple_47:e6:b3 (b0:be:83:47:e6:b3), Dst: zte_ab:73:2c (28:77:77:ab:73:2c) 0010 00 40 00 00 40 00 40
> Internet Protocol Version 4, Src: 192.168.2.41, Dst: 104.16.45.99 0020 2d 63 d4 c0 00 50 85
  0100 .... = Version: 4 0030 ff ff ab 6e 00 00 02
  .... 0101 = Header Length: 20 bytes (5) 0040 00 0a 9d 62 83 10 06
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 64
  Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: TCP (6)
  Header Checksum: 0xe273 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.41
  Destination Address: 104.16.45.99
  [Stream index: 3]
  < Transmission Control Protocol, Src Port: 54464, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 54464
    Destination Port: 80
    [Stream index: 0]
    [Stream Packet Number: 1]
    > [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0 (relative sequence number)
    Sequence Number (raw): 2289022293
    [Next Sequence Number: 1 (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    1011 .... = Header Length: 44 bytes (11)
    > Flags: 0x002 (SYN)
      Window: 65535
      [Calculated window size: 65535]
      Checksum: 0xab6e [unverified]
      [Checksum Status: Unverified]
      Window Offset: 0
    Destination Address (ip.dst), 4 bytes

```

The destination IP address of the SYN packet correspond to one IP address provided in the DNS response message: 104.16.45.99

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
  - Yes. My host issued new DNS queries before the images were retrieved.
11. What is the destination port for the DNS query message? What is the source port of DNS response message?

```
> Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 1
> Ethernet II, Src: Apple_47:e6:b3 (b0:be:83:47:e6:b3), Dst: zte_ab:73:2c (28:77:77:ab:73:2c)
> Internet Protocol Version 4, Src: 192.168.2.41, Dst: 192.168.2.253
User Datagram Protocol, Src Port: 50893, Dst Port: 53
  Source Port: 50893
  Destination Port: 53
  Length: 37
  Checksum: 0x9ec5 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 1]
  [Timestamps]
  UDP payload (29 bytes)
  Domain Name System (query)
    Transaction ID: 0xc0b9
    > 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: 3]
```

Destination port for the DNS query message: 53

```
> Frame 3: 456 bytes on wire (3648 bits), 456 bytes captured (3648 bits) on interface en0,
> Ethernet II, Src: zte_ab:73:2c (28:77:77:ab:73:2c), Dst: Apple_47:e6:b3 (b0:be:83:47:e6:b3)
> Internet Protocol Version 4, Src: 192.168.2.253, Dst: 192.168.2.41
User Datagram Protocol, Src Port: 53, Dst Port: 50893
  Source Port: 53
  Destination Port: 50893
  Length: 422
  Checksum: 0x96fe [unverified]
  [Checksum Status: Unverified]
  [Stream index: 0]
  [Stream Packet Number: 2]
  [Timestamps]
  UDP payload (414 bytes)
  Domain Name System (response)
    Transaction ID: 0xc0b9
    > Flags: 0x8100 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 8
    Additional RRs: 8
  Queries
    > www.mit.edu: type A, class IN
  Answers
  Authoritative nameservers
  Additional records
  [Request In: 2]
  [Time: 0.101941000 seconds]
```

Source port of the DNS response message: 53

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



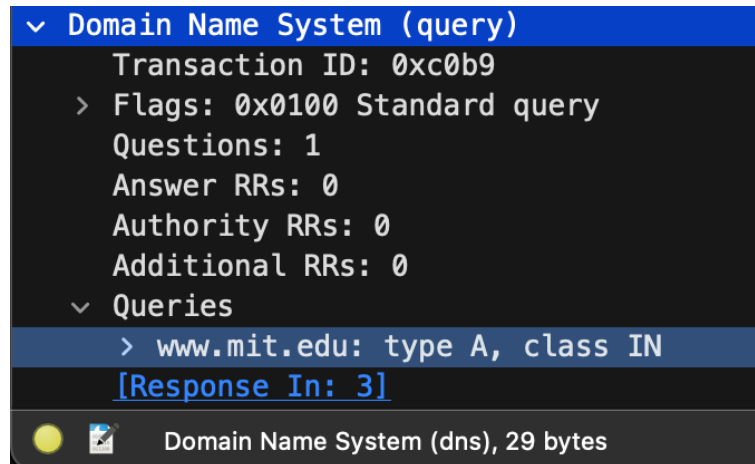
```
> Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface en0, id 1
> Ethernet II, Src: Apple_47:e6:b3 (b0:be:83:47:e6:b3), Dst: zte_ab:73:2c (28:77:77:ab:73:2c)
  ✓ Internet Protocol Version 4, Src: 192.168.2.41, Dst: 192.168.2.253
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 57
      Identification: 0xd26b (53867)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 64
      Protocol: UDP (17)
      Header Checksum: 0x21d2 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.2.41
      Destination Address: 192.168.2.253
      [Stream index: 1]
  ✓ User Datagram Protocol, Src Port: 50893, Dst Port: 53
    Source Port: 50893
    Destination Port: 53
    Length: 37
    Checksum: 0x9ec5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 1]
    > [Timestamps]
    UDP payload (29 bytes)
```

The DNS query message was sent to this IP address: 192.168.2.253

```
dkhoa@192 ~ % cat /etc/resolv.conf
#
# macOS Notice
#
# This file is not consulted for DNS hostname resolution, address
# resolution, or the DNS query routing mechanism used by most
# processes on this system.
#
# To view the DNS configuration used by this system, use:
#   scutil --dns
#
# SEE ALSO
#   dns-sd(1), scutil(8)
#
# This file is automatically generated.
#
nameserver 192.168.2.253
dkhoa@192 ~ %
```

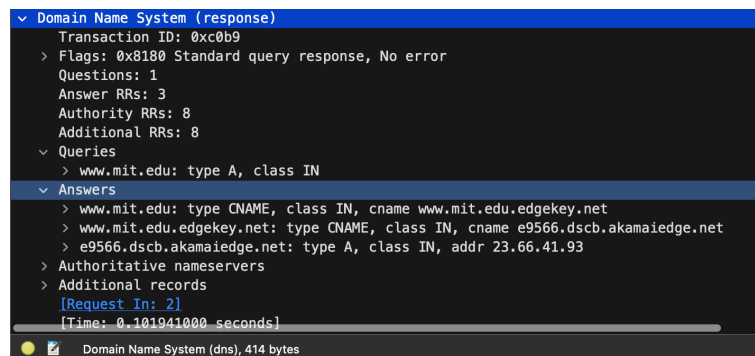
Yes that is my default local DNS server IP address

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



DNS query type: type A. There was no "answer" in the query

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



There are 3 answers in the DNS response message

- The answers contain the following web servers information
  - www.mit.edu
  - www.mit.edu.edgekey.net
  - e9566.dscb.akamaiedge.net

15. Provide a screenshot.

- Provided above

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

```
Internet Protocol Version 4, Src: 192.168.2.41, Dst: 192.168.2.253
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 53
  Identification: 0x64e9 (25833)
  > 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x8f58 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.41
  Destination Address: 192.168.2.253
  [Stream index: 1]
```

The DNS query message was sent to this IP address: 192.168.2.253. Yes, that is my default local DNS server address

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

```
Domain Name System (query)
  Transaction ID: 0x2b3d
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > mit.edu: type NS, class IN
    [Response In: 6]
```

DNS query type: type NS. There was no “answer” in the query

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?

```

v Domain Name System (response)
  Transaction ID: 0x2b3d
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 8
    Authority RRs: 0
    Additional RRs: 7
  > Queries
v Answers
  > mit.edu: type NS, class IN, ns use5.akam.net
  > mit.edu: type NS, class IN, ns ns1-37.akam.net
  > mit.edu: type NS, class IN, ns asia1.akam.net
  > mit.edu: type NS, class IN, ns use2.akam.net
  > mit.edu: type NS, class IN, ns asia2.akam.net
  > mit.edu: type NS, class IN, ns ns1-173.akam.net
  > mit.edu: type NS, class IN, ns usw2.akam.net
  > mit.edu: type NS, class IN, ns eur5.akam.net
  > Additional records
    [Request In: 5]
    [Time: 0.051008000 seconds]

```

MIT nameservers provided by the response message. No, there wasn't any IP address provided

19. Provide a screenshot.

- Provided above

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?

```

v Internet Protocol Version 4, Src: 192.168.2.41, Dst: 18.0.72.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x8a72 (35442)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xd36a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.41
    Destination Address: 18.0.72.3
    [Stream index: 1]

```

The query was sent to 18.0.72.3

- No. It is not my default local DNS server.
- The IP address 18.0.72.3 corresponds to a server within the MIT (Massachusetts Institute of Technology) network, determined by using 'whois 18.0.72.3' lookup in the terminal.

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

```
Domain Name System (query)
> Transaction ID: 0x5f18
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
> Queries
  > www.aiit.or.kr: type A, class IN
```

DNS query type: type A. There was no "answer" in the query

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

```
Domain Name System (response)
  Transaction ID: 0x7bf6
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  > Answers
    > bitsy.mit.edu: type A, class IN, addr 18.0.72.3
      [Request In: 2]
      [Time: 0.049984000 seconds]
```

There is one answer in the response, which is an A record mapping bitsy.mit.edu to the IP address 18.0.72.3

23. Provide a screenshot.

- Provided above