

# Wireshark Lab : DNS

17011588 노하윤

17011599 안정연

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

```
mac — -bash — 80x24
Last login: Mon Oct 14 14:05:12 on ttys000
[(base) nohayun-ui-MacBookAir:~ mac$ nslookup www.asdu.ait.ac.th ]
Server:      164.124.107.9
Address:     164.124.107.9#53

Non-authoritative answer:
www.asdu.ait.ac.th      canonical name = www.misu.ait.ac.th.
Name:   www.misu.ait.ac.th
Address: 203.159.12.3

(base) nohayun-ui-MacBookAir:~ mac$
```

We queried the webpage for the Asian Institute of Technology in Thailand. The IP address of that server was 164.124.107.9

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

```
mac — -bash — 80x24
Last login: Mon Oct 14 14:07:52 on ttys000
[(base) nohayun-ui-MacBookAir:~ mac$ nslookup -type=NS www.cam.ac.uk ]
Server:      164.124.107.9
Address:     164.124.107.9#53

Non-authoritative answer:
*** Can't find www.cam.ac.uk: No answer

Authoritative answers can be found from:
cam.ac.uk
    origin = primary.dns.cam.ac.uk
    mail addr = hostmaster.cam.ac.uk
    serial = 1571029311
    refresh = 1800
    retry = 900
    expire = 604800
    minimum = 3600

(base) nohayun-ui-MacBookAir:~ mac$
```

We used the webpage for Cambridge University in England. This webpage is <http://www.cam.ac.uk>. The authoritative DNS server is [authdns0.csx.ac.uk](http://authdns0.csx.ac.uk).

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?

```
mac — -bash — 80x24
Last login: Mon Oct 14 14:12:22 on ttys000
(base) nohayun-ui-MacBookAir:~ mac$ nslookup www.cam.ac.uk mail.yahoo.com
;; connection timed out; no servers could be reached

(base) nohayun-ui-MacBookAir:~ mac$
```

The IP address for the DNS server if queried for the Yahoo! mail server is 209.191.122.42

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

The image shows a Wireshark packet capture of a DNS query and response. The packet list at the top shows a query (No. 288) and a response (No. 292) between 172.16.31.179 and 164.124.101.2. The packet details for the response (No. 292) are expanded, showing it is a User Datagram Protocol (UDP) message. The source port is 14670 and the destination port is 53. The length is 38 bytes. The checksum is 0xf16b [unverified]. The stream index is 145. The domain name system (query) is shown as 'www.ietf.org'.

The DNS query and response messages are sent over UDP.

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

The image shows the packet details for the DNS response message (No. 292). The source port is 14670 and the destination port is 53. The length is 38 bytes. The checksum is 0xf16b [unverified]. The stream index is 145. The domain name system (query) is shown as 'www.ietf.org'.

The destination port is 53

The source port is 14670

**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?**

224.0.0.251	MDNS	425	Standard query response 0x0000 PTR \35
224.0.0.251	MDNS	425	Standard query response 0x0000 PTR \35
164.124.101.2	DNS	72	Standard query 0xdd2b A www.ietf.org
172.16.31.179	DNS	149	Standard query response 0xdd2b A www.i
104.20.1.85	TCP	78	50081 → 80 [SYN] Seq=0 Win=65535 Len=0
104.20.1.85	TCP	78	50082 → 80 [SYN] Seq=0 Win=65535 Len=0
172.16.31.179	TCP	66	80 → 50081 [SYN, ACK] Seq=0 Ack=1 Win=
104.20.1.85	TCP	54	50081 → 80 [ACK] Seq=1 Ack=1 Win=26214
172.16.31.179	TCP	66	80 → 50082 [SYN, ACK] Seq=0 Ack=1 Win=
104.20.1.85	TCP	54	50082 → 80 [ACK] Seq=1 Ack=1 Win=26214
104.20.1.85	HTTP	495	GET / HTTP/1.1

The DNS query was sent to IP address 164.124.101.2.

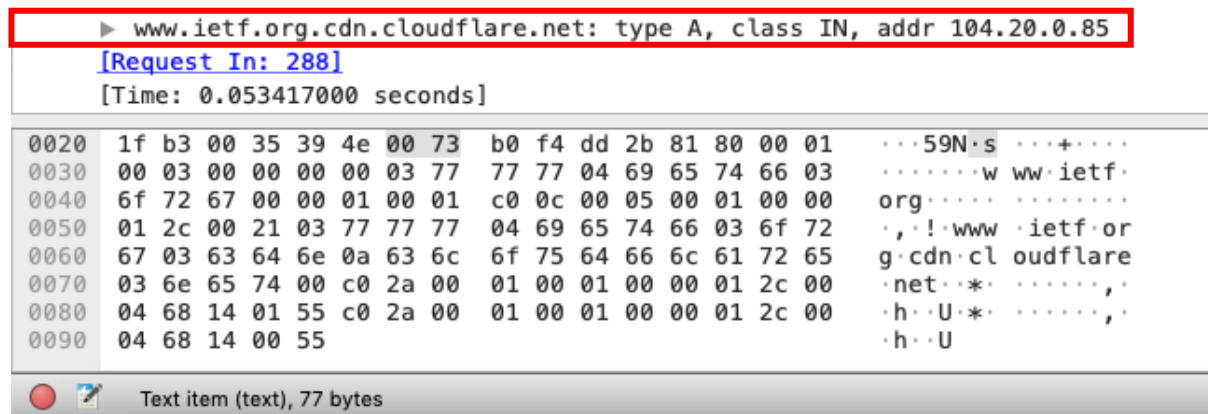
Yes it is the same IP address as that of my local DNS server.

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

```
► Internet Protocol Version 4, Src: 172.16.31.179, Dst: 164.124.101.2
► User Datagram Protocol, Src Port: 14670, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0xdd2b
  ► 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: 292]
```

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

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 [104.20.0.85]. Although it also provided 6 authoritative nameservers, and 11 other responses containing additional 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?

The destination of the SYN packet is [104.20.0.85], the same address that was provided in the DNS response message as the type “A” address of the webpage.

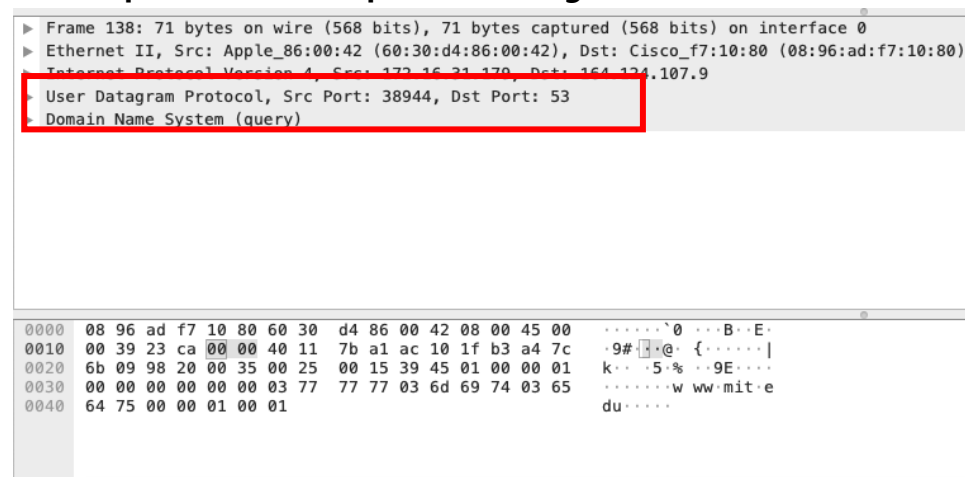
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

ip.addr == 172.16.31.179

No.	Time	Source	Destination	Protocol	Length	Info
43	11:24:25.875948	172.16.31.179	224.0.0.251	MDNS	425	Standard query response 0x0000 PTR
118	11:24:27.742783	172.16.31.179	224.0.0.251	MDNS	425	Standard query response 0x0000 PTR
194	11:24:29.774669	172.16.31.179	224.0.0.251	MDNS	425	Standard query response 0x0000 PTR
238	11:24:31.001901	172.16.31.179	224.0.0.251	MDNS	425	Standard query response 0x0000 PTR
288	11:24:32.308447	172.16.31.179	164.124.101.2	DNS	72	Standard query 0xdd2b A www.ietf.o
292	11:24:32.361864	164.124.101.2	172.16.31.179	DNS	149	Standard query response 0xdd2b A w
293	11:24:32.368529	172.16.31.179	104.20.1.85	TCP	78	50081 → 80 [SYN] Seq=0 Win=65535 L
294	11:24:32.369500	172.16.31.179	104.20.1.85	TCP	78	50082 → 80 [SYN] Seq=0 Win=65535 L
295	11:24:32.374154	104.20.1.85	172.16.31.179	TCP	66	80 → 50081 [SYN, ACK] Seq=0 Ack=1
296	11:24:32.374254	172.16.31.179	104.20.1.85	TCP	54	50081 → 80 [ACK] Seq=1 Ack=1 Win=2
297	11:24:32.374427	104.20.1.85	172.16.31.179	TCP	66	80 → 50082 [SYN, ACK] Seq=0 Ack=1
298	11:24:32.374470	172.16.31.179	104.20.1.85	TCP	54	50082 → 80 [ACK] Seq=1 Ack=1 Win=2
299	11:24:32.374784	172.16.31.179	104.20.1.85	HTTP	495	GET / HTTP/1.1
300	11:24:32.379638	104.20.1.85	172.16.31.179	TCP	60	80 → 50081 [ACK] Seq=1 Ack=442 Win=
301	11:24:32.390826	104.20.1.85	172.16.31.179	TCP	776	80 → 50081 [PSH, ACK] Seq=1 Ack=44
302	11:24:32.390841	104.20.1.85	172.16.31.179	HTTP	60	HTTP/1.1 302 Found (text/html)

Yes, my host did issue new DNS queries before the images were retrieved. For example, one such query was for an image from open-stand.org. The image corresponding to the page was not returned until this query was made.

## 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 : 38944

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

Source	Destination	Protocol	Length	Info
172.16.31.179	224.0.0.251	MDNS	448	Standard query response 0x0000 PTR \
172.16.31.179	224.0.0.251	MDNS	448	Standard query response 0x0000 PTR \
172.16.31.179	224.0.0.251	MDNS	425	Standard query response 0x0000 PTR \
172.16.31.179	164.124.107.9	DNS	71	Standard query 0x3945 A www.mit.edu
164.124.107.9	172.16.31.179	DNS	464	Standard query response 0x3945 A www
172.16.31.179	104.76.91.79	TCP	78	50869 → 80 [SYN] Seq=0 Win=65535 Len
172.16.31.179	104.76.91.79	TCP	78	50870 → 80 [SYN] Seq=0 Win=65535 Len
104.76.91.79	172.16.31.179	TCP	74	80 → 50869 [SYN, ACK] Seq=0 Ack=1 Wi
172.16.31.179	104.76.91.79	TCP	66	50869 → 80 [ACK] Seq=1 Ack=1 Win=131
172.16.31.179	104.76.91.79	HTTP	506	GET / HTTP/1.1
104.76.91.79	172.16.31.179	TCP	74	80 → 50870 [SYN, ACK] Seq=0 Ack=1 Wi
172.16.31.179	104.76.91.79	TCP	66	50870 → 80 [ACK] Seq=1 Ack=1 Win=131
104.76.91.79	172.16.31.179	TCP	66	80 → 50869 [ACK] Seq=1 Ack=441 Win=3
104.76.91.79	172.16.31.179	TCP	1514	80 → 50869 [ACK] Seq=1 Ack=441 Win=3
104.76.91.79	172.16.31.179	TCP	1514	80 → 50869 [ACK] Seq=1449 Ack=441 Wi
104.76.91.79	172.16.31.179	TCP	1514	80 → 50869 [ACK] Seq=2007 Ack=441 Wi

The DNS query message is sent to IP address [164.124.107.9], the same address as my default local DNS server.

**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.

```
▶ Internet Protocol Version 4, Src: 172.16.31.179, Dst: 16
▶ User Datagram Protocol, Src Port: 38944, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x3945
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▼ www.mit.edu: type A, class IN
      Name: www.mit.edu
```

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

```
▶ Answers
  ▼ Authoritative nameservers
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n5dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n7dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n2dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n0dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n4dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n3dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n6dscb.akamaiedge.net
    ▶ dscb.akamaiedge.net: type NS, class IN, ns n1dscb.akamaiedge.net
  ▶ Additional records
    [Request In: 138]
    [Time: 0.006571000 seconds]
```

The response message contains one answer to the aforementioned query which is the type "A" address of <http://www.mit.edu> or 18.9.22.169. It also contained information on 3 authoritative nameservers and 3 additional records.

**15. Provide a screenshot.**

```

ip.addr == 172.16.31.179
No.    Time                Source                Destination          Protocol  Length  Info
43    13:14:45.226675      172.16.31.179        224.0.0.251         MDNS      448    Standard query response 0x0000 PTR /353/205/270/355/225/230/354/234/244/354/235/230
60    13:14:46.565649      172.16.31.179        224.0.0.251         MDNS      448    Standard query response 0x0000 PTR /353/205/270/355/225/230/354/234/244/354/235/230
124   13:14:55.128329      172.16.31.179        224.0.0.251         MDNS      425    Standard query response 0x0000 PTR /353/205/270/355/225/230/354/234/244/354/235/230
138   13:14:55.778712      172.16.31.179        164.124.107.9      DNS       71     Standard query response 0x3945 A www.mit.edu.
139   13:14:55.785286      164.124.107.9        172.16.31.179      DNS       484    Standard query response 0x3945 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9
140   13:14:55.785757      172.16.31.179        104.76.91.79       TCP       78     5069 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=826589517 TSecr=0 SACK_I
141   13:14:55.786365      172.16.31.179        104.76.91.79       TCP       78     50870 -> 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=826589517 TSecr=0 SACK_I
142   13:14:55.790584      104.76.91.79         172.16.31.179      TCP       74     80 -> 50695 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=608146
143   13:14:55.790659      172.16.31.179        104.76.91.79       TCP       66     50695 -> 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=826589522 TSecr=608146137
144   13:14:55.790997      172.16.31.179        104.76.91.79       HTTP      506    GET / HTTP/1.1
145   13:14:55.791268      104.76.91.79         172.16.31.179      TCP       74     80 -> 50870 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=608146
146   13:14:55.791324      172.16.31.179        104.76.91.79       TCP       66     50870 -> 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=826589522 TSecr=608146137
147   13:14:55.796048      104.76.91.79         172.16.31.179      TCP       66     80 -> 50869 [ACK] Seq=1 Ack=441 Win=30000 Len=0 TSval=608146142 TSecr=826589522
152   13:14:55.936286      104.76.91.79         172.16.31.179      TCP       1514   80 -> 50869 [ACK] Seq=1 Ack=441 Win=30000 Len=1448 TSval=608146281 TSecr=826589522
153   13:14:55.936292      104.76.91.79         172.16.31.179      TCP       1514   80 -> 50869 [ACK] Seq=1449 Ack=441 Win=30000 Len=1448 TSval=608146281 TSecr=826589522

Class: IN (0x0001)
  Answers
  Authoritative nameservers
  > dscb.akamaiedge.net: type NS, class IN, ns n5dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n7dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n2dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n0dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n4dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n3dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n6dscb.akamaiedge.net
  > dscb.akamaiedge.net: type NS, class IN, ns n1dscb.akamaiedge.net
  Additional records
  [Request In: 138]

0040  64 75 00 01 00 01 00 01 00 01 00 05 00 05 00 01 00 00 06  du-----
0050  e6 00 19 03 77 77 77 77 03 6d 69 74 03 65 64 75 07  ....www.mit.edu
0060  65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05  ....edgekey.net..
0070  00 01 00 00 00 01 1a 00 18 0e 65 39 35 36 36 04 64  ..e9566-d
0080  73 63 62 8a 61 66 61 6d 61 69 65 64 67 65 0c 3d  scb-akamaiedge=
0090  c0 4e 01 01 00 01 00 00 00 14 00 04 68 4c 5b 4f  ..N.....-lllo
00a0  c0 54 00 02 00 01 00 00 08 80 00 09 06 6e 35 64  ..T.....n5d
00b0  73 63 62 c0 59 c0 54 00 02 00 01 00 08 80 00 00  scb-Y-T.....

```

**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 164.124.107.9, the same IP address as that of my default local DNS server.

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

The DNS query is a type "NS" message including one question. The query message did not contain any answers.

**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?**

The response message provides 3 MIT nameservers :  
w20ns.mit.edu[18.70.0.160] , strawb.mit.edu[18.1.0.150]  
bitsy.mit.edu[18.72.0.3].

The IP addresses for the nameservers was included under the additional records category sent back as part of the response message.



**19. Provide a screenshot.**

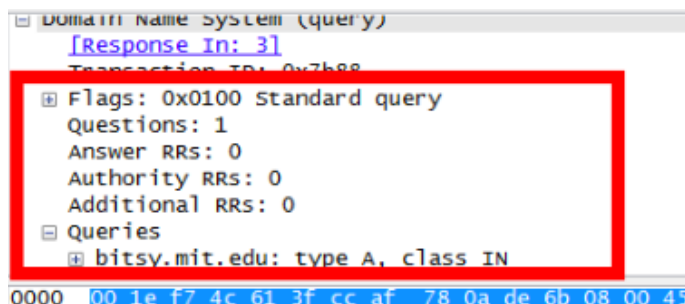
Protocol	Length	Info
DNS	73	Standard query 0x7b88 A bitsy.mit.edu
DNS	73	Standard query 0x7b88 A bitsy.mit.edu
DNS	89	Standard query response 0x7b88 A 18.72.0.3
DNS	82	Standard query 0x0001 PTR 3.0.72.18.in-addr.arpa
DNS	212	Standard query response 0x0001 PTR BITSY.MIT.EDU
DNS	89	Standard query 0x0002 A www.aift.org.kr.easternct.edu
DNS	144	Standard query response 0x0002 No such name
DNS	89	Standard query 0x0003 AAAA www.aift.org.kr.easternct.edu
DNS	144	Standard query response 0x0003 No such name
DNS	75	Standard query 0x0004 A www.aift.org.kr
DNS	191	Standard query response 0x0004 A 222.231.8.226
DNS	75	Standard query 0x0005 AAAA www.aift.org.kr
DNS	139	Standard query response 0x0005
ARP	42	who has 10.36.43.254? Tell 10.36.41.43
ARP	42	10.36.43.254 is at 00:1e:f7:4c:61:3f

**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 149.152.136.65 which is the IP address of the MIT DNS response sender.

**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 answer.



**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.



```

..... 1... .. = Recursion available: Server can do recursive queries
..... 0... .. = 2: RESERVED (0)
..... 0... .. = Answer authenticated: Answer/authority portion was not authenticated
..... 0... .. = Non-authenticated data: Unacceptable
..... 0000 = Reply code: No error (0)

Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

Queries
  bitsy.mit.edu: type A, class IN

Answers
  bitsy.mit.edu: type A, class IN, addr 18.72.0.3

```

**23. Provide a screenshot.**

```

Domain Name System (query)
  [Response in: 3]
  Transaction ID: 0x7b88
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
0000  00 1e f7 4c 61 3f cc af 78 0a de 6b 08 00 45 00  ...La?...x...k...E...
0010  00 3b 37 79 00 00 80 11 b2 10 0a 24 29 2b 95 98  ...?y.....$)+...
0020  88 41 e1 bc 00 35 00 27 96 f0 7b 88 01 00 00 01  ...A...5...{.....
0030  00 00 00 00 00 00 05 62 69 74 73 79 03 6d 69 74  .....b  itsy.mit
0040  03 65 64 75 00 00 01 00 01  .....edu.....

```