20132927_정재명_HW4

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

아시아의 웹사이트 네이버의 아이피 주소를 구했다.

```
[jm:~$nslookup www.naver.com
Server:         168.126.63.1
Address:        168.126.63.1#53

Non-authoritative answer:
www.naver.com   canonical name = www.naver.com.nheos.com.
Name:   www.naver.com.nheos.com
Address: 210.89.160.88
Name:   www.naver.com.nheos.com
Address: 125.209.222.142
```

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

유럽의 대학교 옥스포드 대학교의 책임 dns서버 아이피 주소를 구했다.

```
Authoritative answers can be found from:
ns2.ja.net      internet address = 193.63.105.17
dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
auth4.dns.ox.ac.uk      internet address = 45.33.127.156
auth5.dns.ox.ac.uk      internet address = 93.93.128.67
auth6.dns.ox.ac.uk      internet address = 185.24.221.32
ns2.ja.net      has AAAA address 2001:630:0:45::11
auth4.dns.ox.ac.uk      has AAAA address 2600:3c00::f03c:91ff:fe96:beac
auth5.dns.ox.ac.uk      has AAAA address 2a00:1098:0:80:1000::10
auth6.dns.ox.ac.uk      has AAAA address 2a02:2770:11::21a:4aff:febe:759b
```

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?

다음과 같이 명령어를 입력해보았지만, 거절되거나 time-out 되었다고만 나왔다. 옥스포드 대학 이외에도 십여개의 유럽에 있는 대학 dns 서버의 도메인을 입력해보았지만 같은 결과가 되풀이 되었다.

```
[jm:~$nslookup yahoo.com auth4.dns.ox.ac.uk
Server:         auth4.dns.ox.ac.uk
Address:        45.33.127.156#53

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

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

udp

o.	Time	Source	Destination	Protocol
1	0.000000	192.168.0.2	168.126.63.1	DNS
3	0.432865	168.126.63.1	192.168.0.2	DNS
6	0.436628	192.168.0.2	168.126.63.1	DNS
12	0.446928	168.126.63.1	192.168.0.2	DNS
28	0.501139	192.168.0.2	168.126.63.1	DNS
31	0.512189	168.126.63.1	192.168.0.2	DNS

-> 모두 udp다.

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

- 쿼리 메세지의 소스 포트는 47875이고, 응답 메세지의 소스 포트는 53이다.

```
User Datagram Protocol, Src Port: 53, Dst Port: 47875
    Source Port: 53
```

```
User Datagram Protocol, Src Port: 8480, Dst Port: 53
    Source Port: 8480
```

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?

28	0.501139	192.168.0.2	168.126.63.1	DNS

```
nameserver 168.126.63.1
```

-> 정확히 일치한다.

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

- type A / 어떤 특별한 answers를 가지고 있지는 않다.

```
▼ Queries
  ▼ ssl.gstatic.com: type A, class IN
      Name: ssl.gstatic.com
      [Name Length: 15]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  [Response In: 31]
```

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

- 하나의 답변이 있고, 책임 DNS서버의 아이피주소가 포함되어 있다.

```
▼ Answers
  ▶ ssl.gstatic.com: type A, class IN, addr 216.58.197.131
```

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?

tcp && ip.addr==216.58.197.131

No.	Time	Source	Destination	Protocol	Length	Info
32	0.512356	192.168.0.2	216.58.197.131	TCP	78	53497 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=
47	0.550300	216.58.197.131	192.168.0.2	TCP	74	443 → 53497 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 S
48	0.550355	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=39114937
49	0.550609	192.168.0.2	216.58.197.131	TLSv1.3	643	Client Hello
66	0.587736	216.58.197.131	192.168.0.2	TCP	66	443 → 53497 [ACK] Seq=1 Ack=578 Win=61440 Len=0 TSval=2073469
67	0.588465	216.58.197.131	192.168.0.2	TLSv1.3	278	Server Hello, Change Cipher Spec, Application Data
68	0.588508	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=578 Ack=213 Win=131072 Len=0 TSval=3911
69	0.589525	192.168.0.2	216.58.197.131	TLSv1.3	130	Change Cipher Spec, Application Data
70	0.589702	192.168.0.2	216.58.197.131	TLSv1.3	152	Application Data
71	0.589890	192.168.0.2	216.58.197.131	TLSv1.3	459	Application Data
74	0.626909	216.58.197.131	192.168.0.2	TLSv1.3	630	Application Data, Application Data
75	0.626976	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=1121 Ack=777 Win=130496 Len=0 TSval=391
76	0.628097	192.168.0.2	216.58.197.131	TLSv1.3	97	Application Data
77	0.632061	216.58.197.131	192.168.0.2	TLSv1.3	97	Application Data
78	0.632105	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=1152 Ack=808 Win=131008 Len=0 TSval=391
86	0.663404	216.58.197.131	192.168.0.2	TLSv1.3	381	Application Data
87	0.663406	216.58.197.131	192.168.0.2	TLSv1.3	171	Application Data, Application Data
88	0.663407	216.58.197.131	192.168.0.2	TLSv1.3	105	Application Data
89	0.663438	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=1152 Ack=1123 Win=130752 Len=0 TSval=39
90	0.663438	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=1152 Ack=1228 Win=130624 Len=0 TSval=39
91	0.663439	192.168.0.2	216.58.197.131	TCP	66	53497 → 443 [ACK] Seq=1152 Ack=1267 Win=130560 Len=0 TSval=39
92	0.664276	192.168.0.2	216.58.197.131	TLSv1.3	105	Application Data
106	0.678143	216.58.197.131	192.168.0.2	TCP	66	443 → 53497 [ACK] Seq=1267 Ack=1152 Win=62720 Len=0 TSval=207
107	0.702003	216.58.197.131	192.168.0.2	TCP	66	443 → 53497 [ACK] Seq=1267 Ack=1191 Win=62720 Len=0 TSval=207

- 위 스크린샷에서 보이듯이, SYN패킷의 아이피와 DNS 응답 메세지에 있는 아이피가 같다.

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

- 그렇지 않았다.

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

질의 메세지의 목적지 포트는 53이다. 응답 메세지의 소스 포트 역시 53이다.

```
User Datagram Protocol, Src Port: 62228, Dst Port: 53
    Source Port: 62228
    Destination Port: 53
```

```
User Datagram Protocol, Src Port: 53, Dst Port: 62228
    Source Port: 53
```

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

- 그렇다.

	Time	Source	Destination	Protoc
76	10.380019	192.168.0.2	168.126.63.1	DNS

```
ljm:~$nslookup server
Server:         168.126.63.1
Address:        168.126.63.1#53
```

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

- type A 이다. answer은 포함하고 있지 않다.

```
▼ Queries
  ▼ www.mit.edu: type A, class IN
      Name: www.mit.edu
      [Name Length: 11]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

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

세 개가 있다. 두 개는 별칭 호스트 네임에 대한 정식 호스트 네임의 정보가 담겨있고, 하나는 호스트 네임의 아이피 주소가 담겨 있다.

```
▼ 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 104.74.184.126
```

15. Provide a screenshot.

- 문제마다 스크린샷을 달았다.

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

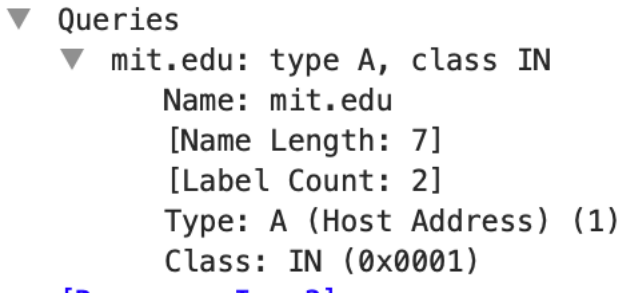
- 같다.

```
  2  1.016908    192.168.0.2          168.126.63.1          DNS
```

```
ljm:~$nslookup server
Server:         168.126.63.1
Address:        168.126.63.1#53
```

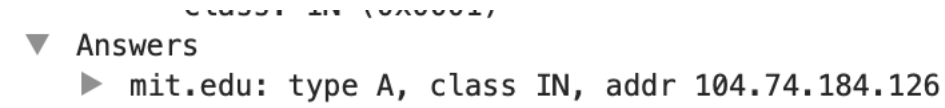
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

- dns 질의문의 type은 A다. 어떠한 answer을 포함하고 있지는 않는다.



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?

- mit.edu 라는 네임 서버가 응답 메세지에 포함되어 왔다. 아이피 주소 또한 포함하고 있다.

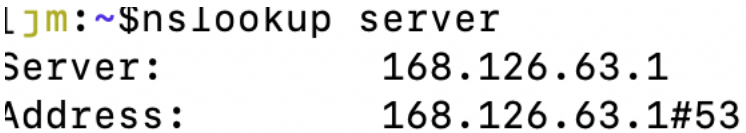


19. Provide a screenshot.

- 문제별로 스크린샷을 달았다.

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?

- 첫번째 메세지는 일치한다. 일치하지 않는 두번째 DNS 메세지의 경우, 첫번째 DNS 응답 메세지에 담겨온 책임 서버의 ip주소와 같다.



```
    7  1.943837    192.168.0.2           18.0.72.3             DNS                74
```

```
▼ Answers
  ▶ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
```

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

- type은 A고, 어떠한 answer도 가지고 있지 않다.

```
▼ Queries
  ▼ www.aiit.or.kr: type A, class IN
      Name: www.aiit.or.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

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

- 책임 DNS 서버의 도메인 이름과 아이피 주소가 포함되어 있다.

```
▼ Answers
  ▶ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
```

23. Provide a screenshot.

- 문제 별로 스크린샷을 달았다.