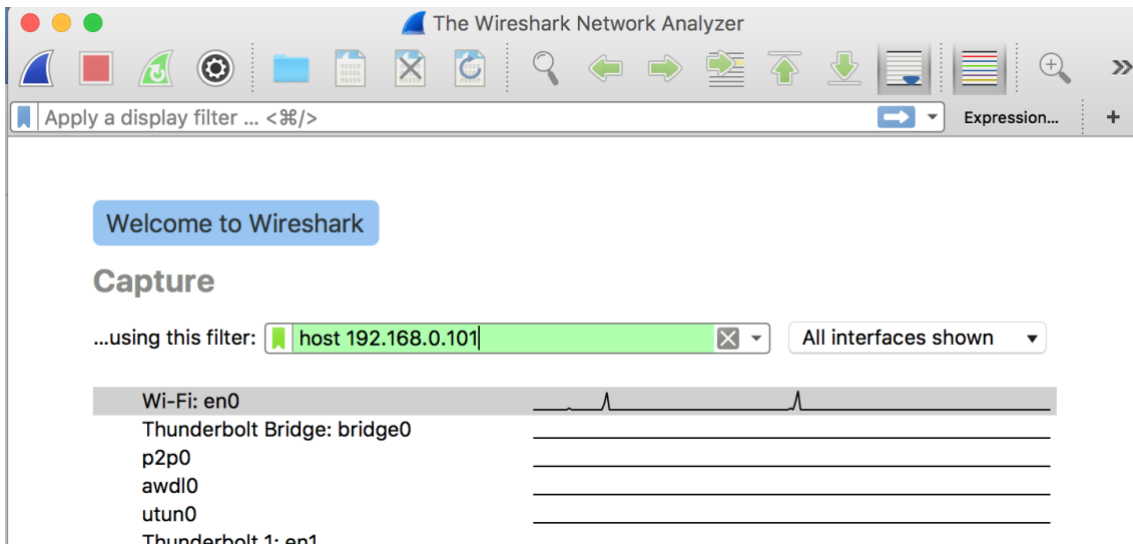
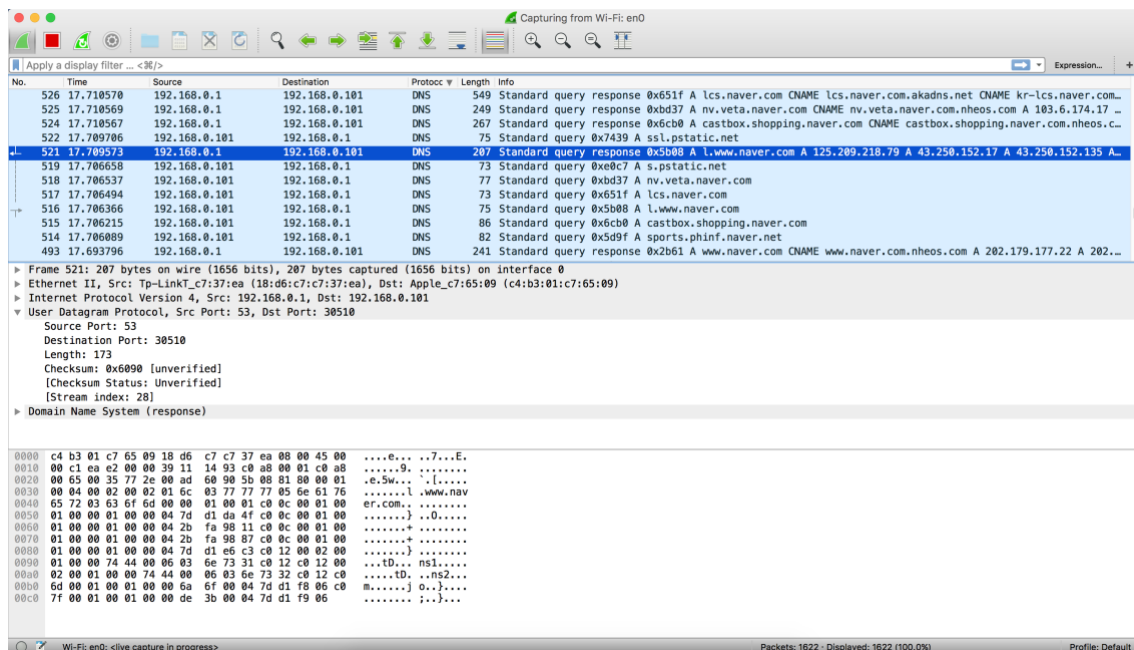


```
sunghyun — sunghyun@Macproui-MacBook-Pro —
nslookup naver.com
Server:      192.168.0.1
Address:     192.168.0.1#53

Non-authoritative answer:
Name:   naver.com
Address: 202.179.177.21
Name:   naver.com
Address: 202.179.177.22
Name:   naver.com
Address: 125.209.222.141
Name:   naver.com
Address: 125.209.222.142
```

<https://www.naver.com> 의 IP address 를 구하였다.





naver.com DNS 가 동작하였을 때의 query 와 response message 를 분석하였다.

▼ User Datagram Protocol, Src Port: 30510, Dst Port: 53

naver.com 은 신뢰성 있는 1:1 전달이 필요한 사이트가 아니므로, 유연하고 효율적으로 데이터 전송이 가능한 UDP(User Datagram Protocol)를 사용하고 있는 것으로 확인하였다.

query 와 response 메시지의 Source 와 Destination Port number

<query message> source port: 30510, destination port: 53

▼ User Datagram Protocol, Src Port: 30510, Dst Port: 53

Source Port: 30510

Destination Port: 53

<response message> source port: 53, destination port: 30510

▼ User Datagram Protocol, Src Port: 53, Dst Port: 30510

Source Port: 53

Destination Port: 30510

DNS 의 well-known Port 번호인 53 을 사용하고 있는 것으로 나타났다.

query와 response 메시지에서 source와 destination IP 주소들을 확인.

<query message>

[Header checksum status: Unverified]

Source: 192.168.0.101

Destination: 192.168.0.1

[Source, Dest IP: Unknown]

query message에서 source IP는 192.168.0.101이며, destination IP는 192.168.0.1이다.

<response message>

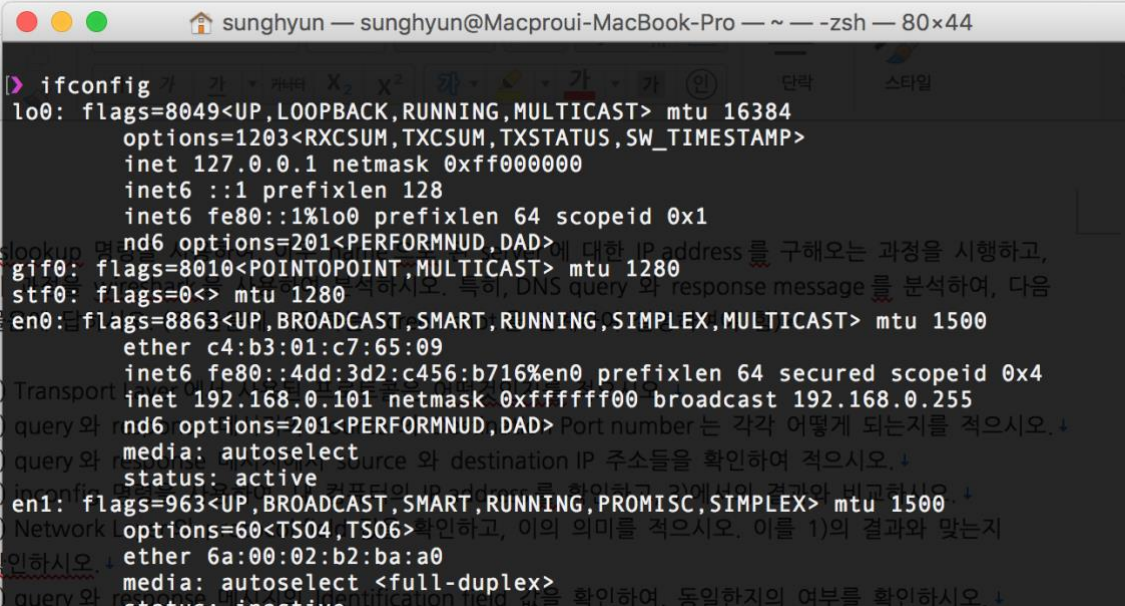
[Header checksum status: Unverified]

Source: 192.168.0.1

Destination: 192.168.0.101

query message에서 source IP는 192.168.0.1이며, destination IP는 192.168.0.101이다.

ifconfig 명령으로 IP address를 확인, 결과 비교



```
sunghyun — sunghyun@Macproui-MacBook-Pro — ~ — zsh — 80x44
[> ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
  options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
  inet 127.0.0.1 netmask 0xff000000
  inet6 ::1 prefixlen 128
  inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
  nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
  ether c4:b3:01:c7:65:09
  inet6 fe80::4dd:3d2:c456:b716%en0 prefixlen 64 secured scopeid 0x4
  inet 192.168.0.101 netmask 0xfffff00 broadcast 192.168.0.255
  nd6 options=201<PERFORMNUD,DAD>
  media: autoselect
  status: active
en1: flags=963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX> mtu 1500
  Options=60<TS04,TS06>
  ether 6a:00:02:b2:ba:a0
  media: autoselect <full-duplex>
  status: inactive
```

source IP는 192.168.0.101로 3과 동일하지만, broadcast는 192.168.0.255로 외부에서 나의 네트워크에 접속하기 위해서 배포되는 IP 주소는 3의 destination IP와는 차이가 나타난다.

Network Layer 의 protocol field 값을 확인.

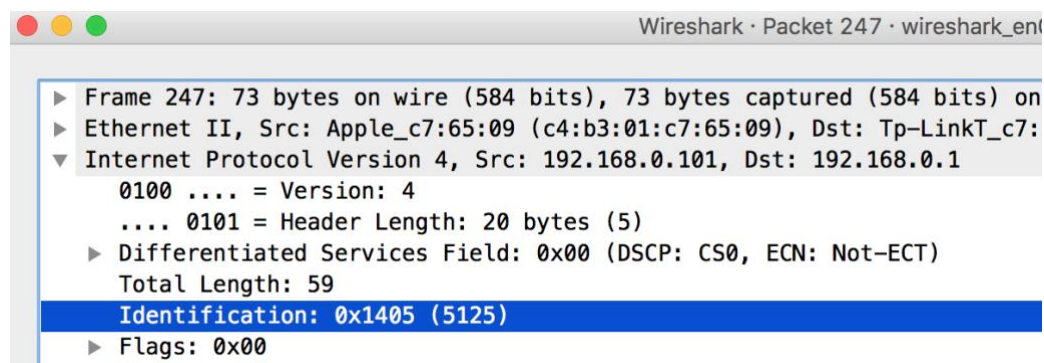


Network Layer 의 Protocol 은 Internet Protocol 중 IPv4(Internet Protocol Version 4)로 나타나며, Header Length 가 20 바이트라는 것은 Transport Layer 의 패킷정보에 20 바이트의 IP header 가 붙어 Network Layer 에 전송되었다는 것을 의미한다.

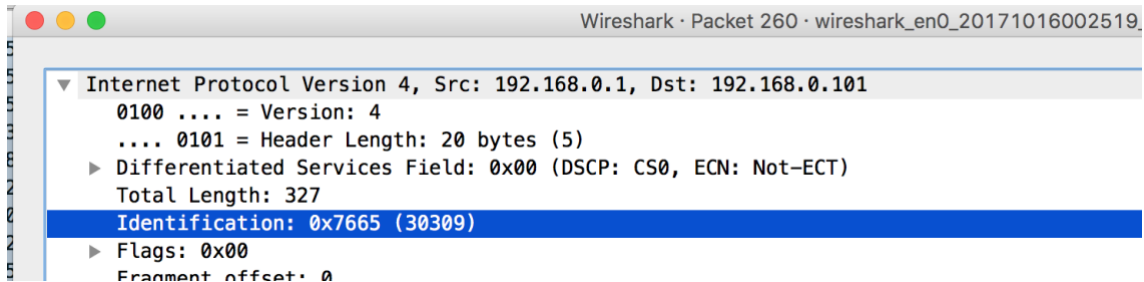
1 에서 본 UDP Header 에는 첫 2 바이트 안에 Source Port 와 Destination Port 가 자리하고 있는데, 이를 전송받은 IPv4 에서도 Src Port 와 Dst Port 가 UDP 속의 Port 와 동일한 것으로 보아 그대로 하위 계층으로 전송되어 Header 만 붙는 형태를 확인할 수 있다.

query 와 response 메시지의 Identification field 값을 확인.

<query message>



<response message>

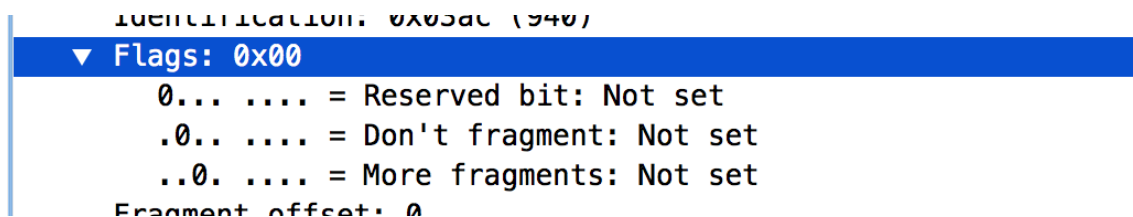


query 와 response 메시지의 Identification field 값은 각각 0x1405(5125), 0x7665(30309)로 같지않다.

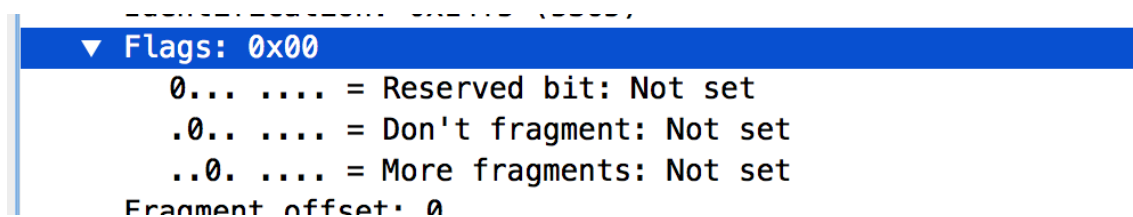
Identification 은 query 와 response 가 동일한 데이터그램에 속하게 되면 같은 일련번호를 공유하게 된다. 하지만, 해당 통신은 UDP 를 사용하여 양방향으로 응답을 확인하며 이루어지는 것이 아니기 때문에 반드시 같은 데이터그램에 속할 수 없는 것으로 확인되어진다.

query 와 response 메시지의 flags field 의 각 값들이 어떻게 되는지 ?

<query message>



<response message>

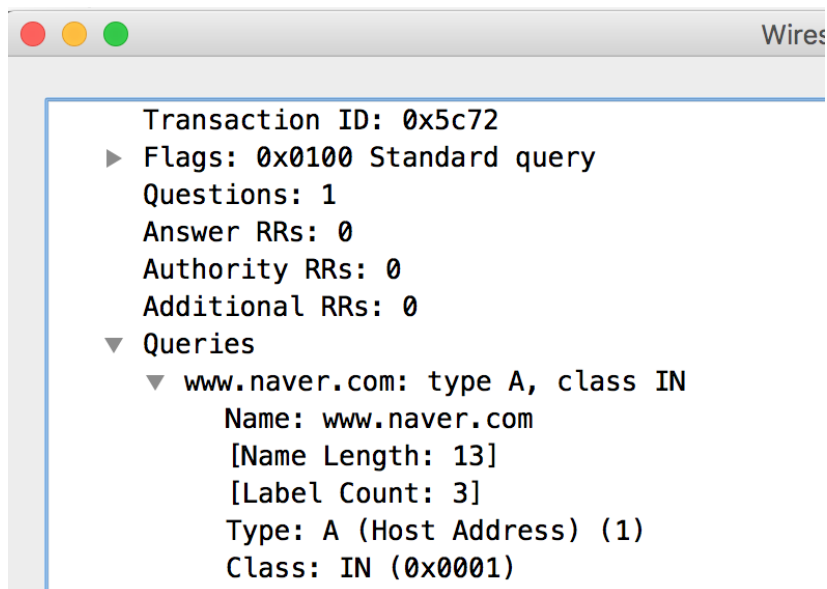


Flags field 는 query 에 대한 여러가지 정보를 갖고 있는 필드로써, 3bit 로 이루어져 있다.

첫번째 bit 는 항상 미사용으로써 0 을 띄고 있다. 두번째 bit 는 분열되어 조각나 있다면, 0 으로 셋팅 되어 라우터에서도 분열이나 단편화가 가능함을 뜻하며, 만약 1 이라면 미분열 상태로써 컴퓨터가 해당 조각들을 다시 합칠 수 없으므로 중간에 라우터가 데이터그램을 단편화하지 말라는 뜻으로 나타난다.

세번째 bit 인 More Fragment 는 현재의 조각이 마지막이라면 0 으로 나타나며, 뒤에 더 많은 조각이 있다면 1 로 나타난다. 위의 사진에서는 0 으로 나타나므로 현재의 조각이 마지막임을 알 수 있다.

query message 에서 question 필드의 내용을 분석..



query message 에서 Questions 필드는 DNS Query 의 이름을 정의하는 역할을 하며 Name, Type, Class 로 구조로 되어있다.

Name 필드는 가변적으로 호스트 이름이 들어간다. 호스트 네임의 영문자를 헥사코드로 변경할 때 이를 구분하기 위해서 숫자로 구분 문자를 넣게 된다. www.naver.com 의 경우 03www05naver03com00 으로 표시된다.

0000	18 d6 c7 c7 37 ea c4 b3 01 c7 65 09 08 00 45 007... ..e...E.
0010	00 3b 42 5a 00 00 40 11 b6 9e c0 a8 00 68 c0 a8	.;BZ..@.h..
0020	00 01 b1 2b 00 35 00 27 0d ed 01 82 01 00 00 01	...+.5.'
0030	00 00 00 00 00 00 03 77 77 77 05 6e 61 76 65 72w ww.naver
0040	03 63 6f 6d 00 00 01 00 01	.com.... .

Type 필드는 쿼리의 유형을 정의하는 것으로, A 는 Host Address 를 나타낸다.

Class 필드는 네트워크의 Class 타입을 표시하는 것으로 일반적으로 IN 클래스를 사용한다.

response message 에서 "answers"의 수와 정보..

```
▼ Answers
  ▼ www.naver.com: type CNAME, class IN, cname www.naver.com.nheos.com
    Name: www.naver.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 2235
    Data length: 22
    CNAME: www.naver.com.nheos.com
  ▼ www.naver.com.nheos.com: type A, class IN, addr 202.179.177.22
    Name: www.naver.com.nheos.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 75
    Data length: 4
    Address: 202.179.177.22
  ▼ www.naver.com.nheos.com: type A, class IN, addr 125.209.222.141
    Name: www.naver.com.nheos.com
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 75
    Data length: 4
    Address: 125.209.222.141
```

answer 의 수는 3 가지로 보여진다. Answer 에는 Name, Type, Class, TTL(Time to Live), Dlength(Data length), Address 로 구성되어 있으며, Name, Type, Class 는 위에 설명한 Question field 의 의미와 동일하다. TTL 은 DNS 응답에 사용된 데이터를 해당 서버가 캐싱 정보로 유지하는 시간을 나타내는 것이다. Data Length 는 데이터의 길이를 나타내며, Address 대신 Data 가 들어가기도 하는데 이는 실제로 전송되고 있는 본래의 실제 정보를 의미한다. 이는 Type 과 Class 에 따라 변화되는 가변 길이를 가지게 된다.

"Number of questions", "Number of answer RRs" 필드를 확인

```
▼ Domain Name System (query)
  [Response In: 428]
  Transaction ID: 0x5c72
  ► Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ► Queries
▼ Domain Name System (response)
  [Request In: 427]
  [Time: 0.001855000 seconds]
  Transaction ID: 0x5c72
  ► Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 3
  Additional RRs: 3
  ► Queries
  ► Answers
  ► Authoritative nameservers
```

Number of questions 는 1 개이고, Number of answer RRs 는 3 개이다. Query 를 요청하는 부분에서는 Answer 가 나타나고 있지 않지만, response query message 에서는 응답수가 3 으로 나타났다는 것은 응답을 해줬기 때문이다. Authority RRs 와 Additional RRs 의 수도 3 으로 나타났다는 것은 공식 DNS 서버와 다른 DNS 서버에서도 응답이 왔다는 것이다.