DNS

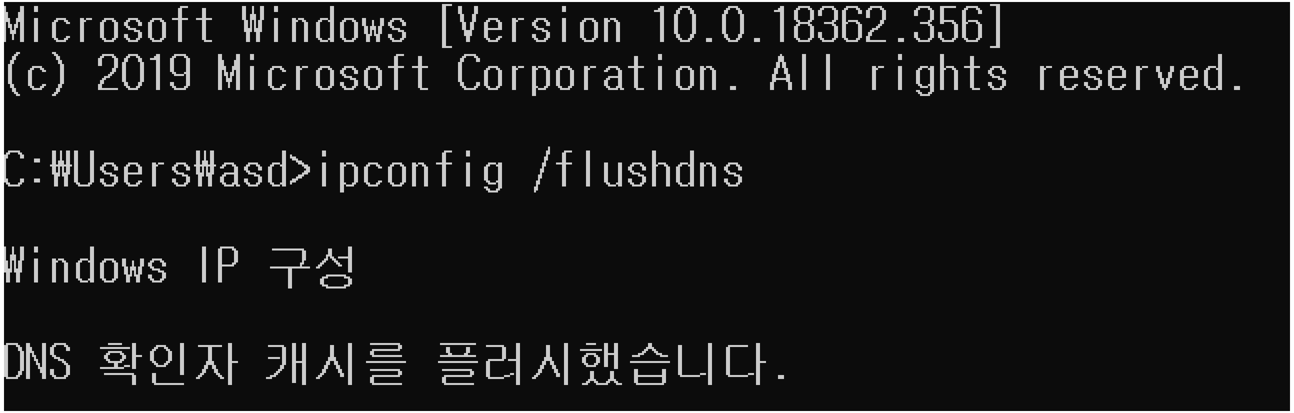
네트워크프로그래밍

휴먼지능정보공학과
201810776 소재휘

#1 ns lookup

Network programming

1.Use ipconfig to empty the DNS cache in your host. ipconfig /flushdns

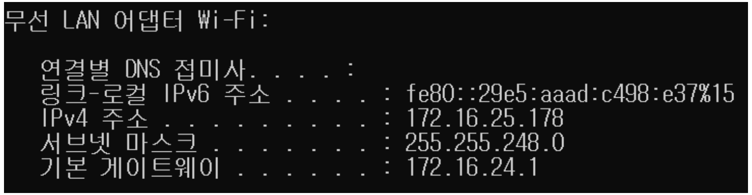


```
Microsoft Windows [Version 10.0.18362.356]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\asd>ipconfig /flushdns

Windows IP 구성

DNS 확인자 캐시를 플러시했습니다.
```

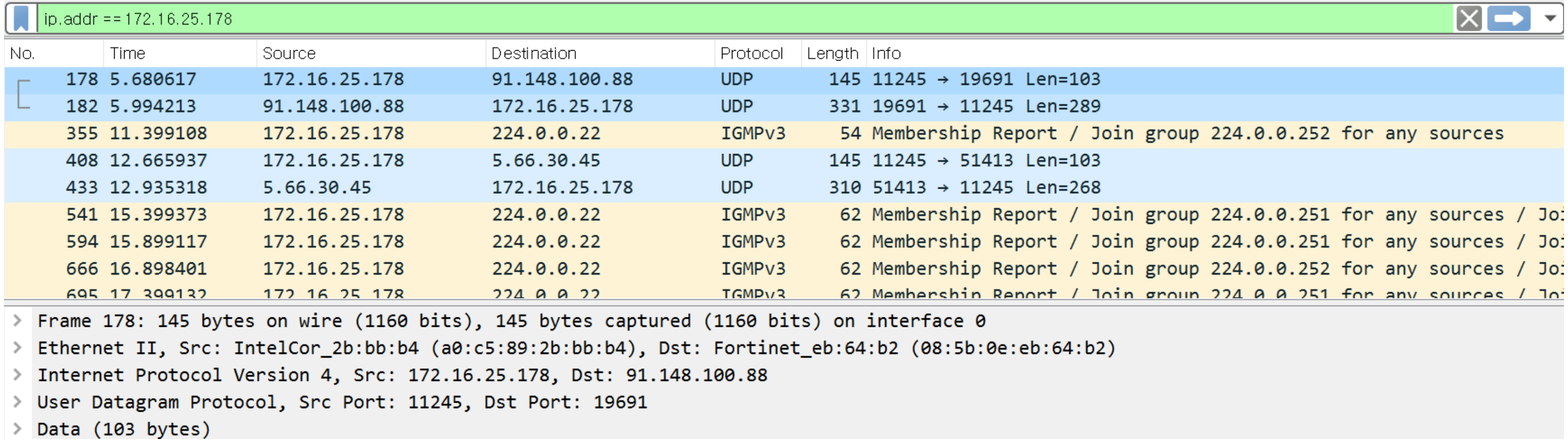
#1 ns lookup

Network programming

2. Open Wireshark and enter “ip.addr == your_IP_address” into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.



```
무선 LAN 어댑터 Wi-Fi:

   연결별 DNS 접미사. . . . :
   링크-로컬 IPv6 주소 . . . . : fe80::29e5:aaad:c498:e37%15
   IPv4 주소 . . . . . . . . . : 172.16.25.178
   서브넷 마스크 . . . . . . . : 255.255.248.0
   기본 게이트웨이 . . . . . . : 172.16.24.1
```



```
ip.addr == 172.16.25.178
```

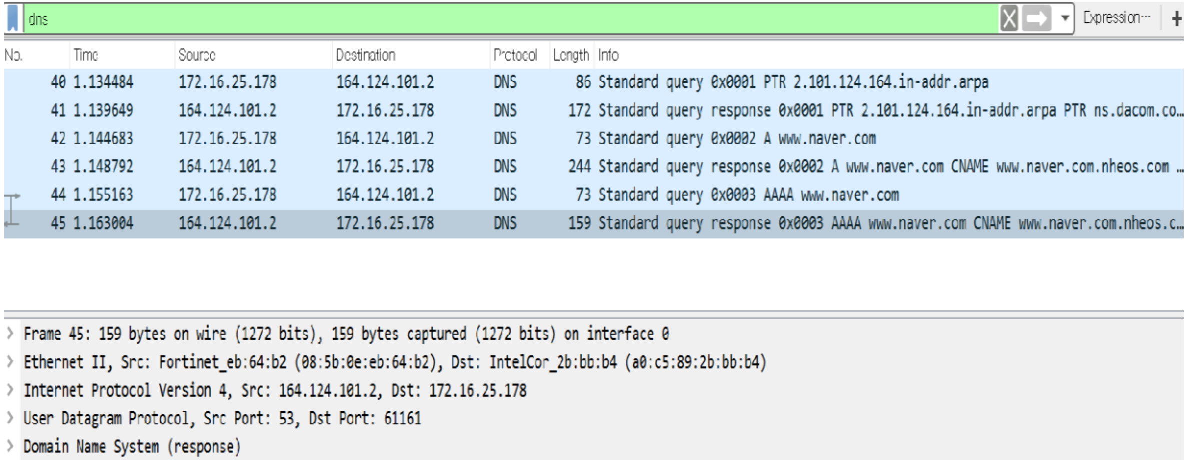
```
No.    Time       Source          Destination    Protocol  Length Info
   178 5.680617   172.16.25.178   91.148.100.88  UDP       145 11245 → 19691 Len=103
   182 5.994213   91.148.100.88   172.16.25.178  UDP       331 19691 → 11245 Len=289
   355 11.399108  172.16.25.178   224.0.0.22     IGMPv3     54 Membership Report / Join group 224.0.0.252 for any sources
   408 12.665937  172.16.25.178   5.66.30.45     UDP       145 11245 → 51413 Len=103
   433 12.935318  5.66.30.45      172.16.25.178  UDP       310 51413 → 11245 Len=268
   541 15.399373  172.16.25.178   224.0.0.22     IGMPv3     62 Membership Report / Join group 224.0.0.251 for any sources / Joi
   594 15.899117  172.16.25.178   224.0.0.22     IGMPv3     62 Membership Report / Join group 224.0.0.251 for any sources / Joi
   666 16.898401  172.16.25.178   224.0.0.22     IGMPv3     62 Membership Report / Join group 224.0.0.252 for any sources / Joi
   695 17.399132  172.16.25.178   224.0.0.22     IGMPv3     62 Membership Report / Join group 224.0.0.251 for any sources / Joi
```

```
> Frame 178: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0
> Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
> Internet Protocol Version 4, Src: 172.16.25.178, Dst: 91.148.100.88
> User Datagram Protocol, Src Port: 11245, Dst Port: 19691
> Data (103 bytes)
```

#1 ns lookup

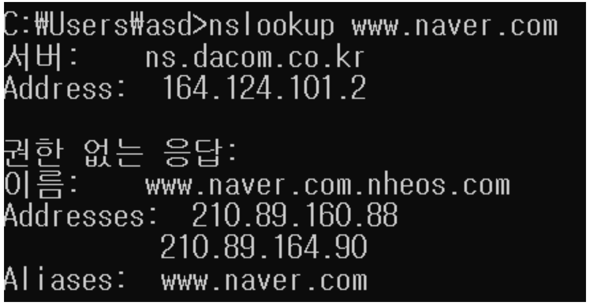
Network programming

3.Before running nslookup in step 4, start capture using Wireshark
4.Open a CMD window and Run “nslookup www.naver.com”



No.	Time	Source	Destination	Protocol	Length	Info
40	1.134484	172.16.25.178	164.124.101.2	DNS	86	Standard query 0x0001 PTR 2.101.124.164.in-addr.arpa
41	1.139649	164.124.101.2	172.16.25.178	DNS	172	Standard query response 0x0001 PTR 2.101.124.164.in-addr.arpa PTR ns.dacom.co…
42	1.144683	172.16.25.178	164.124.101.2	DNS	73	Standard query 0x0002 A www.naver.com
43	1.148792	164.124.101.2	172.16.25.178	DNS	244	Standard query response 0x0002 A www.naver.com CNAME www.naver.com.nheos.com …
44	1.155163	172.16.25.178	164.124.101.2	DNS	73	Standard query 0x0003 AAAA www.naver.com
45	1.163004	164.124.101.2	172.16.25.178	DNS	159	Standard query response 0x0003 AAAA www.naver.com CNAME www.naver.com.nheos.c…

```
> Frame 45: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
> Ethernet II, Src: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2), Dst: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4)
> Internet Protocol Version 4, Src: 164.124.101.2, Dst: 172.16.25.178
> User Datagram Protocol, Src Port: 53, Dst Port: 61161
> Domain Name System (response)
```



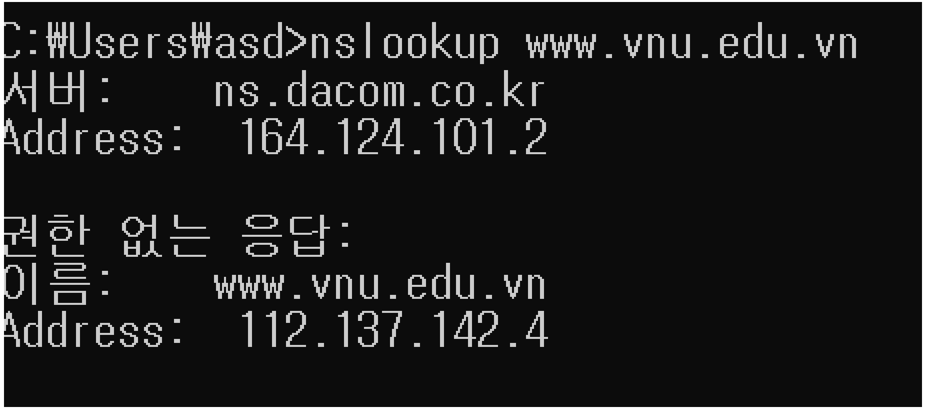
```
C:₩Users₩asd>nslookup www.naver.com
서버:    ns.dacom.co.kr
Address:  164.124.101.2

권한 없는 응답:
이름:    www.naver.com.nheos.com
Addresses:  210.89.160.88
          210.89.164.90
Aliases:  www.naver.com
```

Local DNS Server가 다른 DNS Server의 캐시 정보를 가지고 있어 IP Address를 이미 아는 경우에 바로 해당 서버의 주소를 알 수 있다. 이러한 경우를 권한 없는 응답. Non-authoritative answer이라고 한다.

#1 ns lookup

Network programming

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



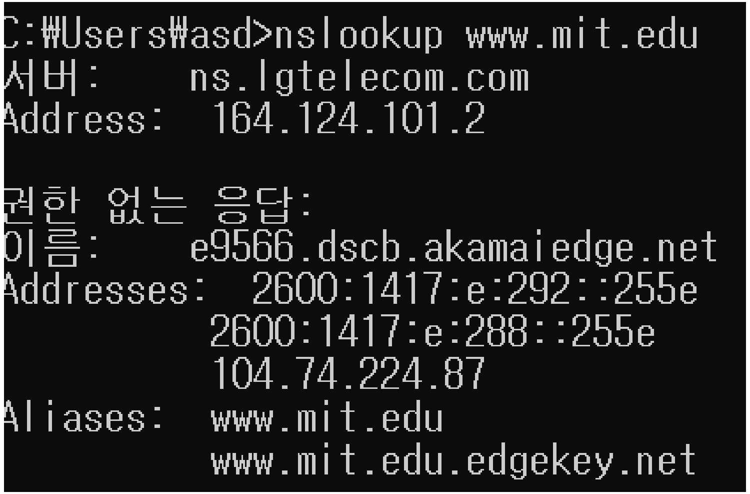
```
C:₩Users₩asd>nslookup www.vnu.edu.vn
서버:    ns.dacom.co.kr
Address:  164.124.101.2

권한 없는 응답:
이름:    www.vnu.edu.vn
Address:  112.137.142.4
```

베트남의 대학교를 nslookup
하였다. IP Address는
112.137.142.4

#2 ns lookup continued

Network programming

Start packet capture.
Do an nslookup on www.mit.edu
Stop packet capture.

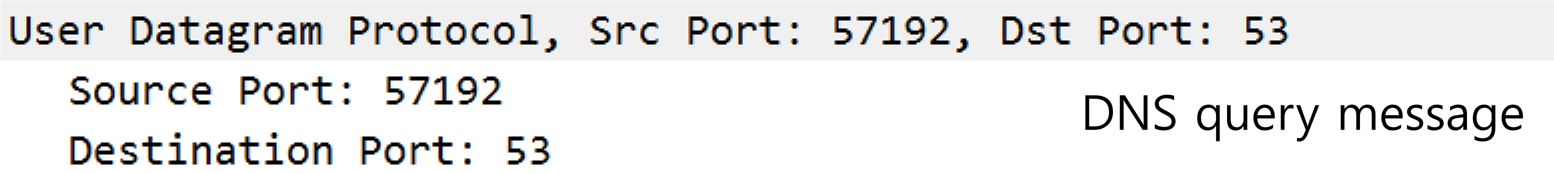


```
C:₩Users₩asd>nslookup www.mit.edu
서버:    ns.lgtelecom.com
Address:  164.124.101.2

권한 없는 응답:
이름:    e9566.dscb.akamaiedge.net
Addresses:  2600:1417:e:292::255e
          2600:1417:e:288::255e
          104.74.224.87
Aliases:  www.mit.edu
          www.mit.edu.edgekey.net
```

#2 ns lookup continued

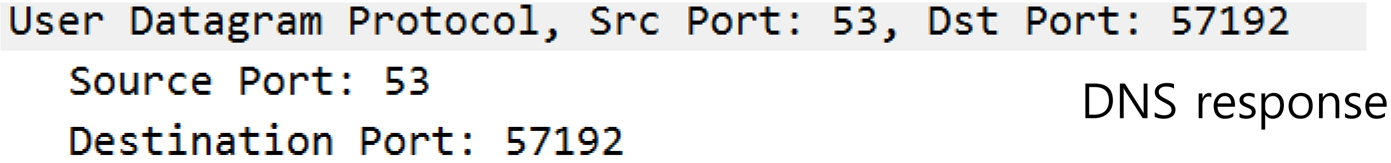
Network programming

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



```
User Datagram Protocol, Src Port: 57192, Dst Port: 53
    Source Port: 57192
    Destination Port: 53
```

DNS query message



```
User Datagram Protocol, Src Port: 53, Dst Port: 57192
    Source Port: 53
    Destination Port: 57192
```

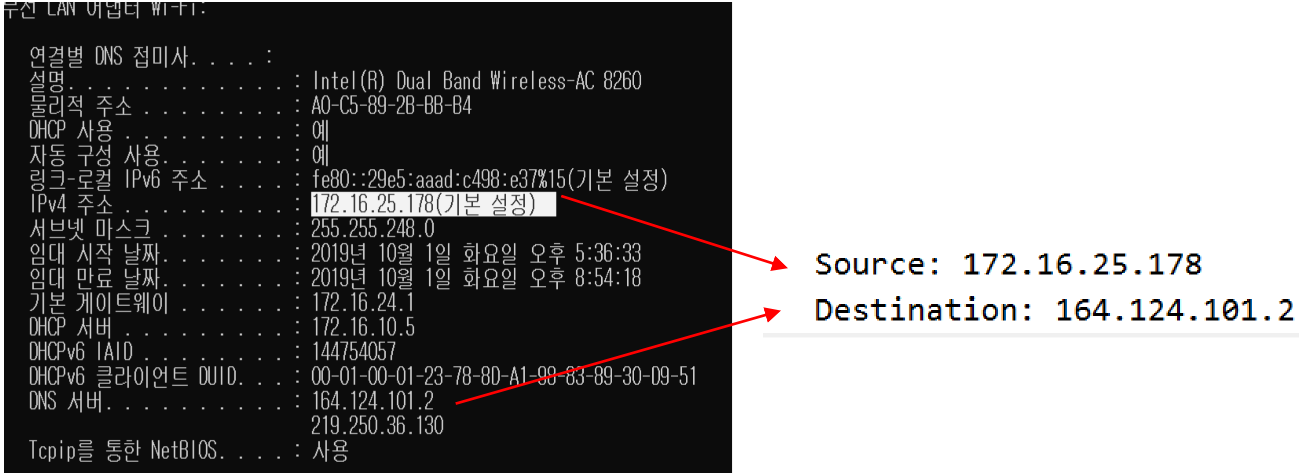
DNS response message

DNS 질의 메시지의 Destination Port는 53
DNS 응답 메시지의 Source Port는 53으로 질의 메시지가 응답 메시지의 포트로 전해진 것을 확인할 수 있다.

#2 ns lookup continued

Network programming

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



```
무선 LAN 어댑터 Wi-Fi:

   연결별 DNS 접미사. . . . :
   설명. . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
   물리적 주소 . . . . . . . . : A0-C5-89-2B-BB-B4
   DHCP 사용 . . . . . . . . . : 예
   자동 구성 사용. . . . . . . : 예
   링크-로컬 IPv6 주소 . . . . : fe80::29e5:aaad:c498:e37%15(기본 설정)
   IPv4 주소 . . . . . . . . . : 172.16.25.178(기본 설정)
   서브넷 마스크 . . . . . . . : 255.255.248.0
   임대 시작 날짜. . . . . . . : 2019년 10월 1일 화요일 오후 5:36:33
   임대 만료 날짜. . . . . . . : 2019년 10월 1일 화요일 오후 8:54:18
   기본 게이트웨이 . . . . . . : 172.16.24.1
   DHCP 서버 . . . . . . . . . : 172.16.10.5
   DHCPv6 IAID . . . . . . . . : 144754057
   DHCPv6 클라이언트 DUID. . . : 00-01-00-01-23-78-8D-A1-98-83-89-30-D9-51
   DNS 서버. . . . . . . . . . : 164.124.101.2
                                 219.250.36.130
   Tcpip를 통한 NetBIOS. . . . : 사용
```

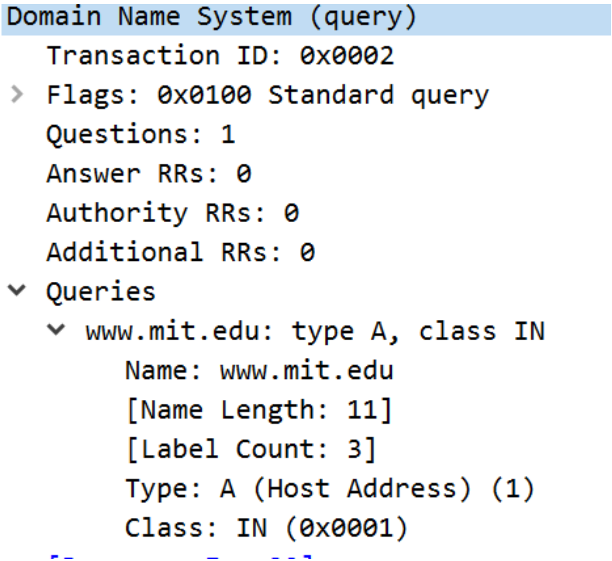
```
Source: 172.16.25.178
Destination: 164.124.101.2
```

DNS 쿼리 메시지의 Destination IP address는 164.124.101.2이다. 이는 기본 로컬 DNS 서버의 IP 주소이다.

#2 ns lookup continued

Network programming

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



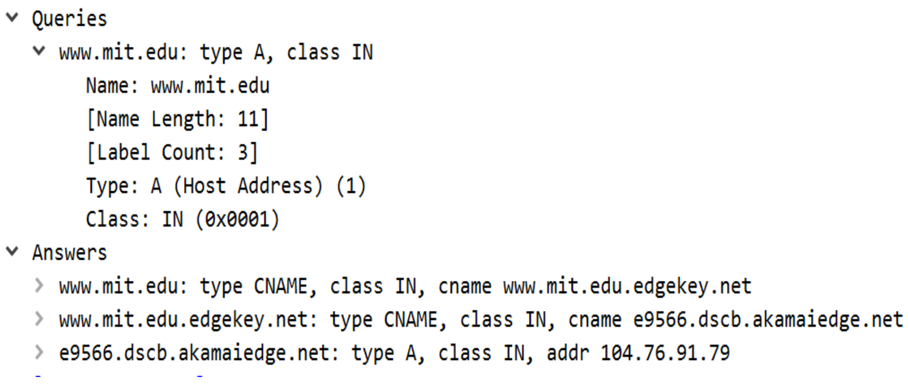
```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⌄ Queries
      ⌄ www.mit.edu: type A, class IN
            Name: www.mit.edu
            [Name Length: 11]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
```

DNS query message의 type은 A이다. 질의 message이므로 answer은 존재하지 않는다.

#2 ns lookup continued

Network programming

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



```
v Queries
  v 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)
v 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 104.76.91.79
```

3개의 Answers들이 있다. 각 Answer의 내용은 다음과 같다.

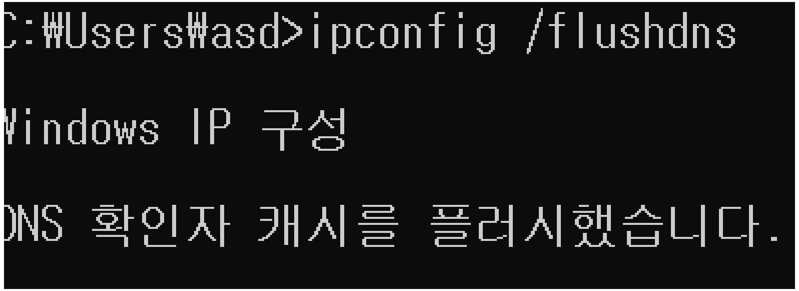
1. www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
   타입 : CNAME, 다음 CNAME의 주소 제공
2. www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaidge.net
   타입 : CNAME, 다음 CNAME의 주소 제공
3. e9566.dscb.akamaidge.net : type A, class IN, addr 104.76.91.79
   타입 :A, IP주소 제공

#3 DNS

Network programming

1.Use ipconfig to empty the DNS cache in your host.

ipconfig /flushdns



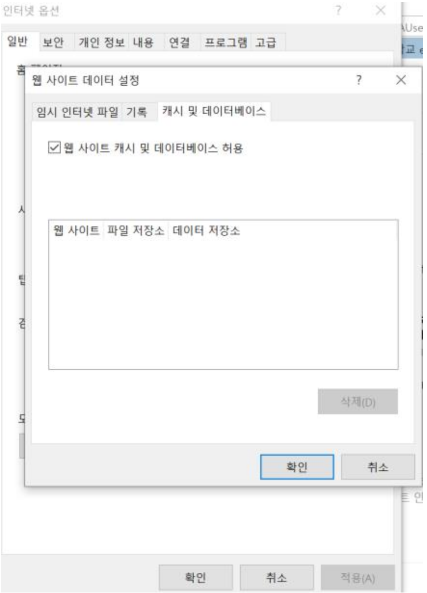
```
C:₩Users₩asd>ipconfig /flushdns

Windows IP 구성

DNS 확인자 캐시를 플러시했습니다.
```

호스트의 DNS 캐시를 비웠다.

#3 DNS

Network programming

2. Open your browser and empty your browser cache. (With Internet Explorer, go to Tools menu and select Internet Options; then in the General tab select Delete Files.)



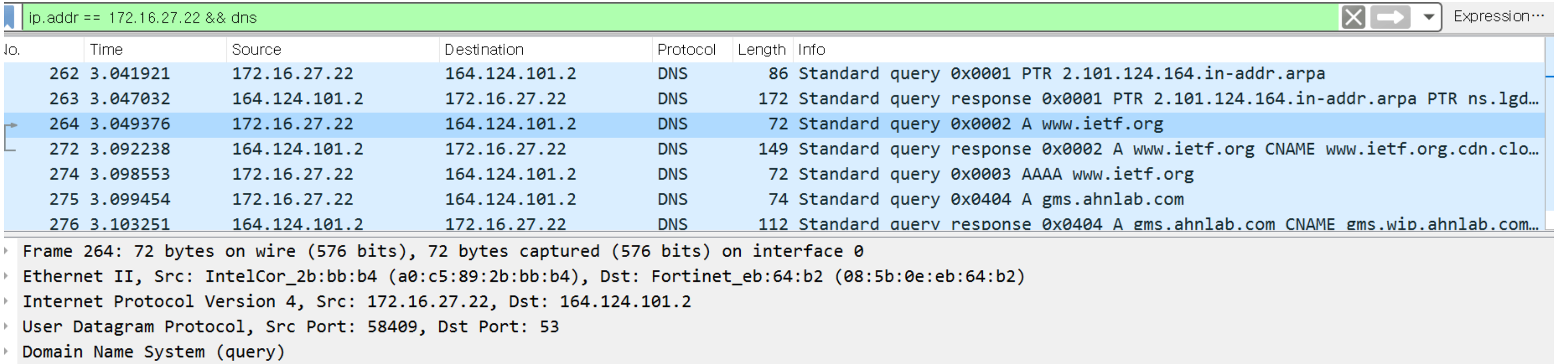
☑ 웹 사이트 캐시 및 데이터베이스 허용

브라우저 캐시를 비웠다.

#3 DNS

Network programming

3. Open Wireshark and enter “ip.addr == your_IP_address” into the filter, where you obtain your_IP_address with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
4. Start packet capture in Wireshark.
5. With your browser, visit the Web page: http://www.ietf.org
6. Stop packet capture.



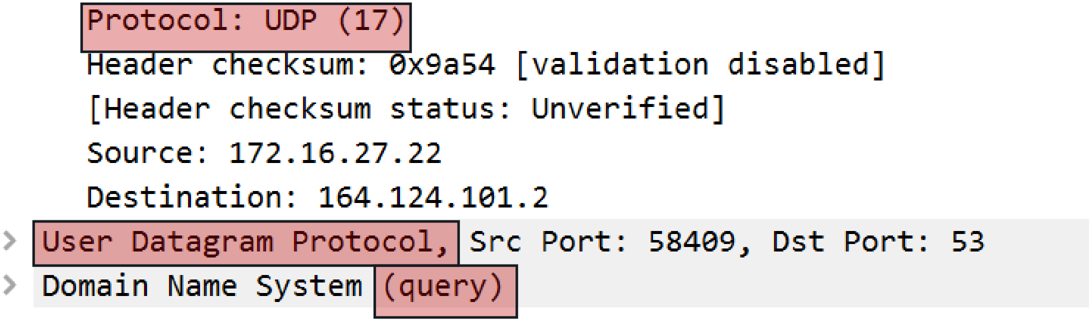
```
ip.addr == 172.16.27.22 && dns

No.   Time      Source         Destination    Protocol Length Info
  262 3.041921  172.16.27.22   164.124.101.2  DNS        86 Standard query 0x0001 PTR 2.101.124.164.in-addr.arpa
  263 3.047032  164.124.101.2  172.16.27.22   DNS       172 Standard query response 0x0001 PTR 2.101.124.164.in-addr.arpa PTR ns.lgd…
  264 3.049376  172.16.27.22   164.124.101.2  DNS        72 Standard query 0x0002 A www.ietf.org
  272 3.092238  164.124.101.2  172.16.27.22   DNS       149 Standard query response 0x0002 A www.ietf.org CNAME www.ietf.org.cdn.clo…
  274 3.098553  172.16.27.22   164.124.101.2  DNS        72 Standard query 0x0003 AAAA www.ietf.org
  275 3.099454  172.16.27.22   164.124.101.2  DNS        74 Standard query 0x0404 A gms.ahnlab.com
  276 3.103251  164.124.101.2  172.16.27.22   DNS       112 Standard query response 0x0404 A gms.ahnlab.com CNAME gms.wip.ahnlab.com…

Frame 264: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
Ethernet II, Src: IntelCor_2b:bb:b4 (a0:c5:89:2b:bb:b4), Dst: Fortinet_eb:64:b2 (08:5b:0e:eb:64:b2)
Internet Protocol Version 4, Src: 172.16.27.22, Dst: 164.124.101.2
User Datagram Protocol, Src Port: 58409, Dst Port: 53
Domain Name System (query)
```

www.ietf.org를 방문 후 나의 ip 주소를
filter처리하여 얻어낸 운 패킷의 목록이다.

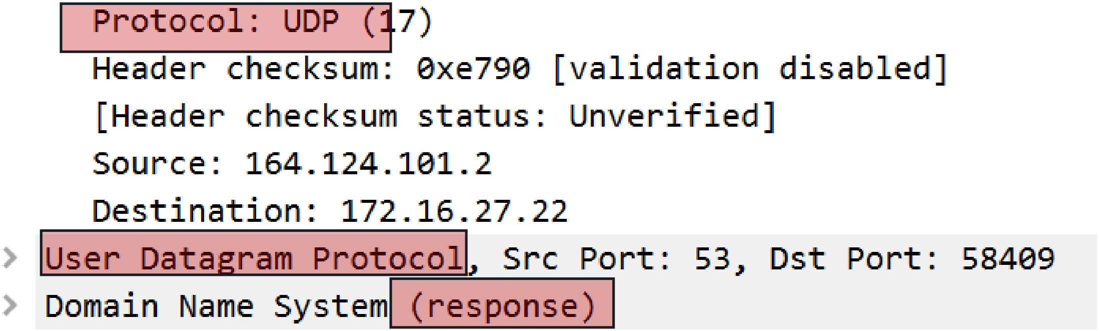
#3 DNS

Network programming

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



```
 Protocol: UDP (17)
 Header checksum: 0x9a54 [validation disabled]
 [Header checksum status: Unverified]
 Source: 172.16.27.22
 Destination: 164.124.101.2
> User Datagram Protocol, Src Port: 58409, Dst Port: 53
> Domain Name System (query)
```



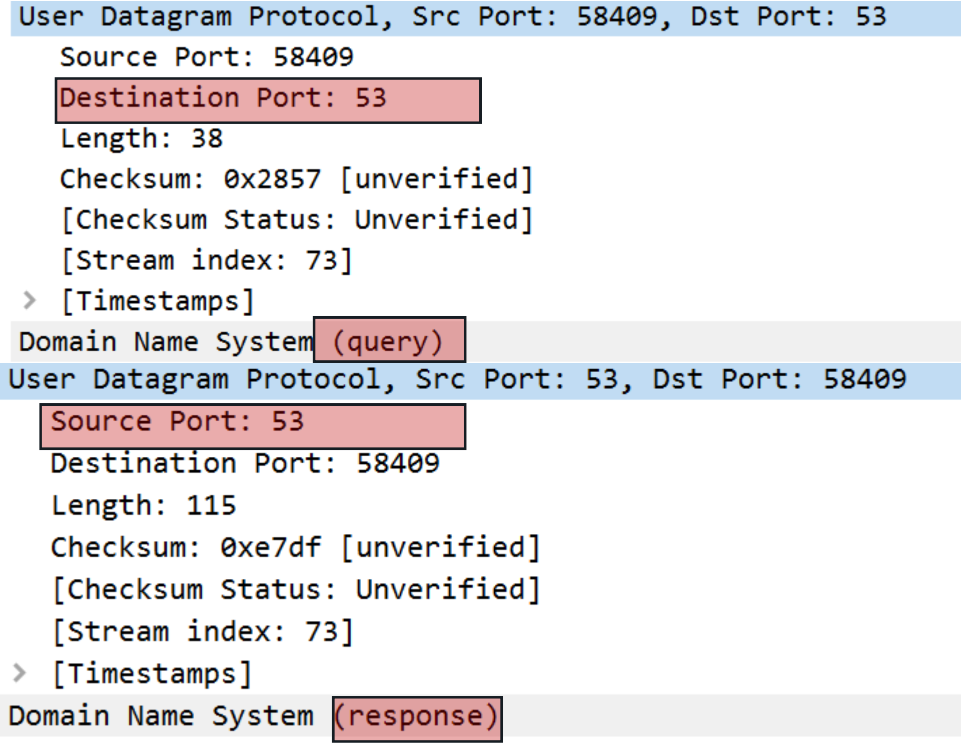
```
 Protocol: UDP (17)
 Header checksum: 0xe790 [validation disabled]
 [Header checksum status: Unverified]
 Source: 164.124.101.2
 Destination: 172.16.27.22
> User Datagram Protocol, Src Port: 53, Dst Port: 58409
> Domain Name System (response)
```

Transport layer의 protocol은 UDP로 UDP를 통해 query와 response를 전송한다.

#3 DNS

Network programming

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



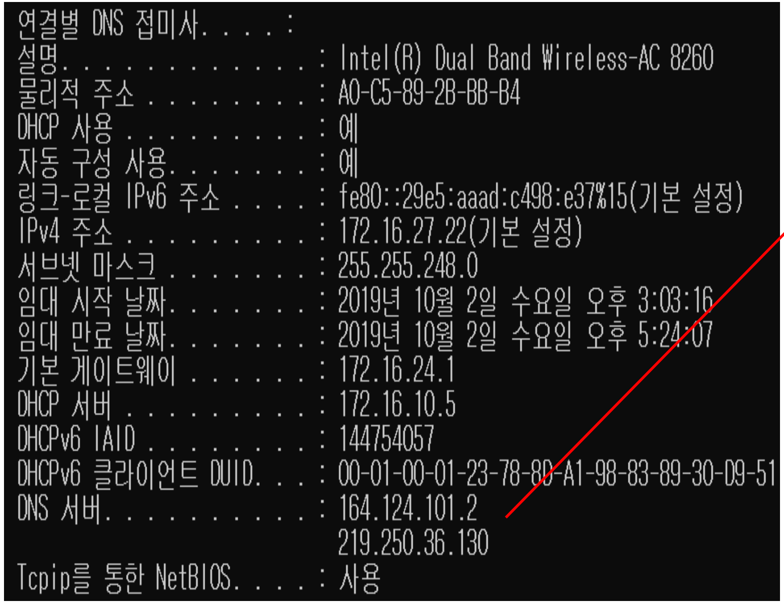
```
User Datagram Protocol, Src Port: 58409, Dst Port: 53
    Source Port: 58409
    Destination Port: 53
    Length: 38
    Checksum: 0x2857 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 73]
  > [Timestamps]
Domain Name System (query)
User Datagram Protocol, Src Port: 53, Dst Port: 58409
    Source Port: 53
    Destination Port: 58409
    Length: 115
    Checksum: 0xe7df [unverified]
    [Checksum Status: Unverified]
    [Stream index: 73]
  > [Timestamps]
Domain Name System (response)
```

DNS query message의
Destination port는 53이고
DNS response message의
Source port는 53으로
질의한 메시지가 응답
메시지의 포트로 전달된
것을 알 수 있다.

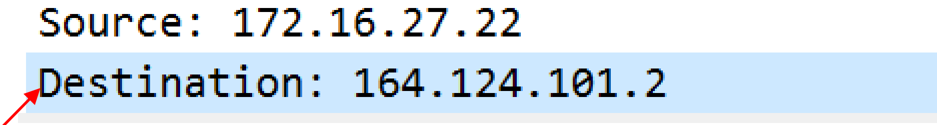
#3 DNS

Network programming

3. 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?



```
연결별 DNS 접미사. . . . :
설명. . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
물리적 주소 . . . . . . . . : A0-C5-89-2B-BB-B4
DHCP 사용 . . . . . . . . . : 예
자동 구성 사용. . . . . . . : 예
링크-로컬 IPv6 주소 . . . . : fe80::29e5:aaad:c498:e37%15(기본 설정)
IPv4 주소 . . . . . . . . . : 172.16.27.22(기본 설정)
서브넷 마스크 . . . . . . . : 255.255.248.0
임대 시작 날짜. . . . . . . : 2019년 10월 2일 수요일 오후 3:03:16
임대 만료 날짜. . . . . . . : 2019년 10월 2일 수요일 오후 5:24:07
기본 게이트웨이 . . . . . . : 172.16.24.1
DHCP 서버 . . . . . . . . . : 172.16.10.5
DHCPv6 IAID . . . . . . . . : 144754057
DHCPv6 클라이언트 DUID. . . : 00-01-00-01-23-78-8D-A1-98-83-89-30-09-51
DNS 서버. . . . . . . . . . : 164.124.101.2
                              219.250.36.130
Tcpip를 통한 NetBIOS. . . . : 사용
```



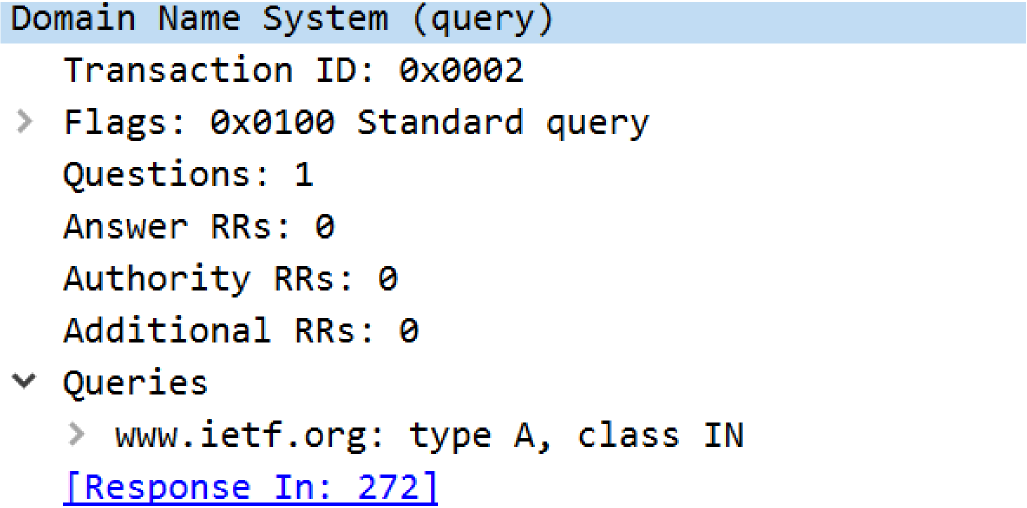
```
Source: 172.16.27.22
Destination: 164.124.101.2
```

DNS query message를 보낼 IP 주소는 기본 로컬 DNS 서버의 IP 주소와 동일하다는 것을 알 수 있다.

#3 DNS

Network programming

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



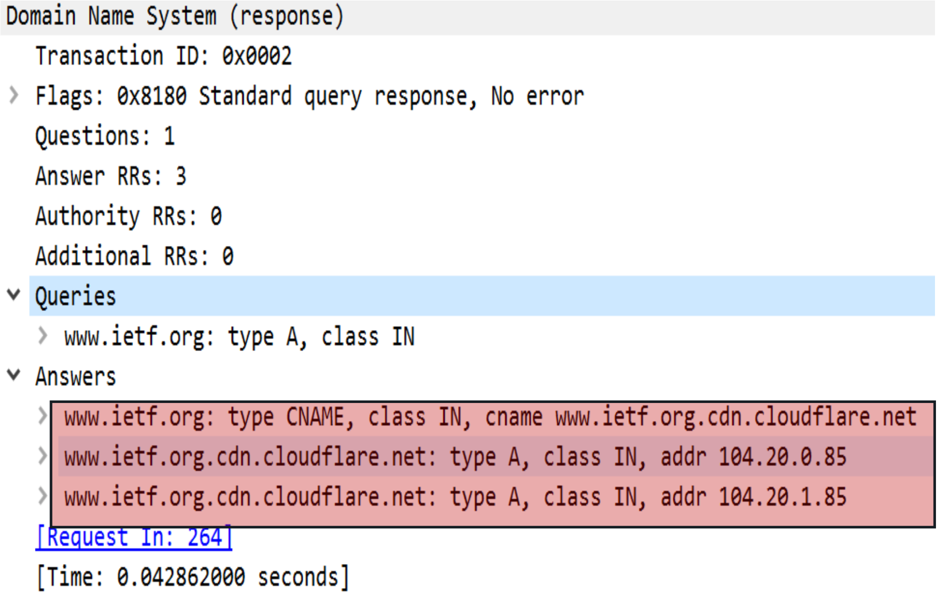
```
Domain Name System (query)
    Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ˅ Queries
      > www.ietf.org: type A, class IN
    [Response In: 272]
```

DNS query의 type은 A이며 질의 메시지 이므로 아무런 응답(answer)도 포함하지 않는다.

#3 DNS

Network programming

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



```
Domain Name System (response)
    Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
      > www.ietf.org: type A, class IN
  v Answers
      > www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
      > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      > www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
    [Request In: 264]
    [Time: 0.042862000 seconds]
```

DNS response message에는 3개의 answer가 있었다.

첫번째 answer에서는 type은 CNAME이고 CNAME www.ietf.org.cdn.cloudflare.net을 명시했다.

두번째 answer에서는 type은 A이고 Address 104.20.0.85을 명시했다.

세번째 answer에서는 type은 A이고 Address 104.20.1.85를 명시했다.