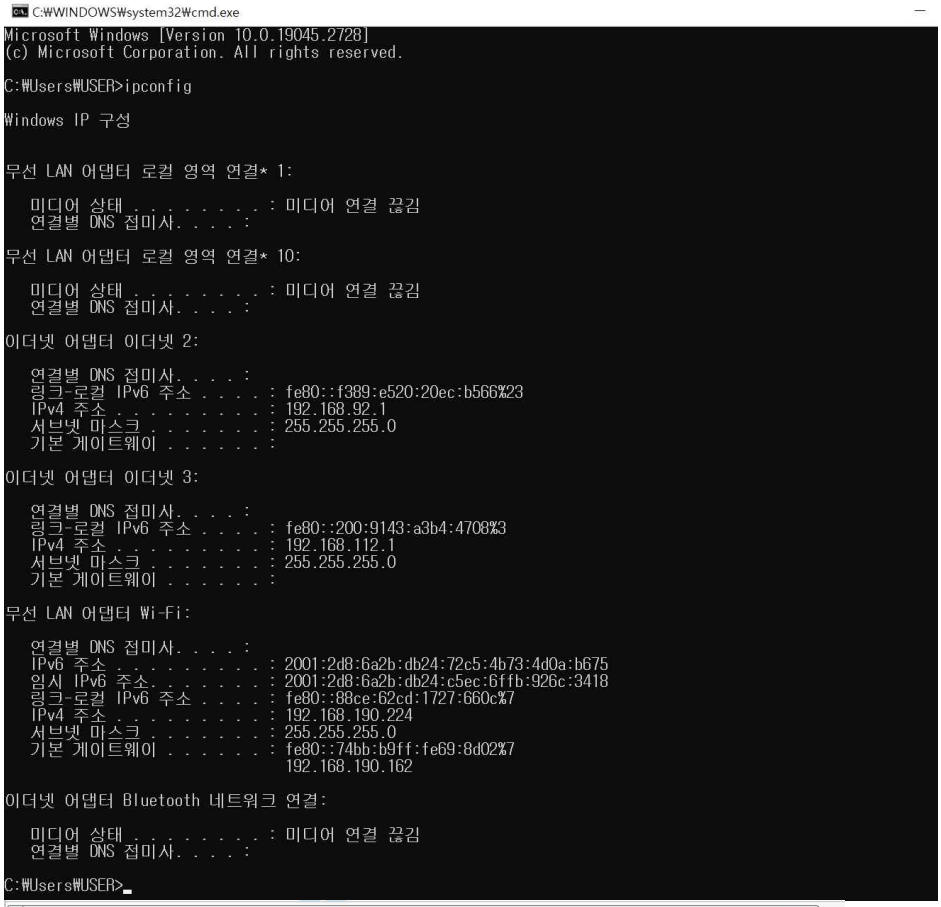
컴퓨터 네트워크
(화5목6)

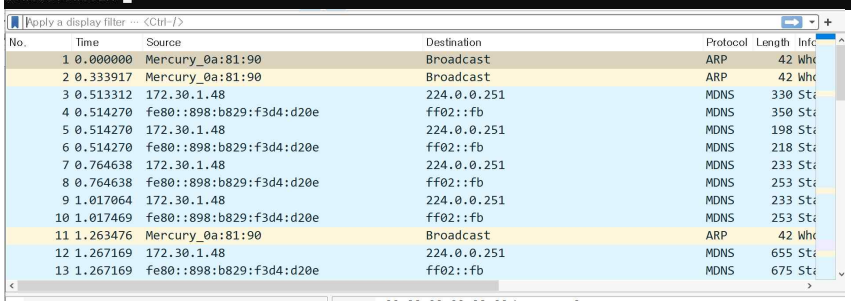
학부:컴퓨터정보공학부
학번:2021202045
이름:김예은
담당 교수님:이혁준 교수님
제출일: 2023.04.10.

서론

wireshark라는 sniffer 프로그램을 이용하여 packet을 캡처하고 packet을 분석한다. 먼저, wireshark 프로그램을 다운받고, 사용법을 간단히 익힌다. 이 프로그램을 이용하여 http와 dns에 대해 분석하면서 http와 dns에 대한 실습을 진행한다. 교재에 제시되어 있는 링크를 접속하고, cmd를 이용하여 ip 주소나 DNS local server를 확인한다. 새로운 링크를 열기 전 항상 캐쉬를 지워주는 작업을 한다.

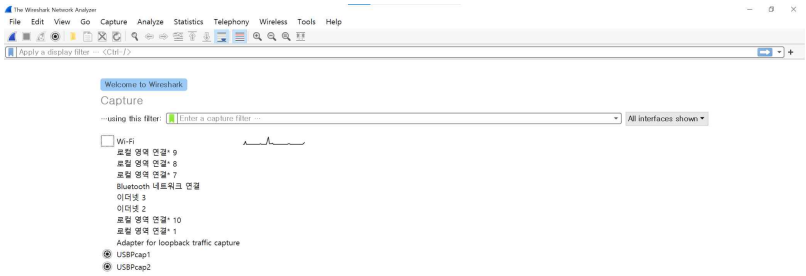
Ⅰ. Question #1

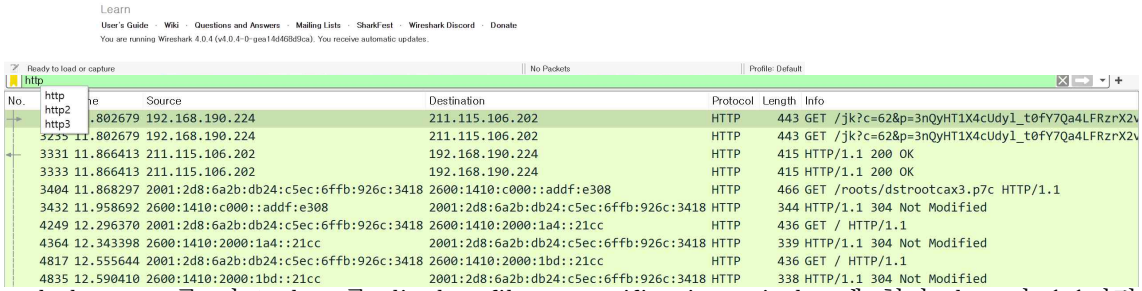




Ⅱ. Question #2

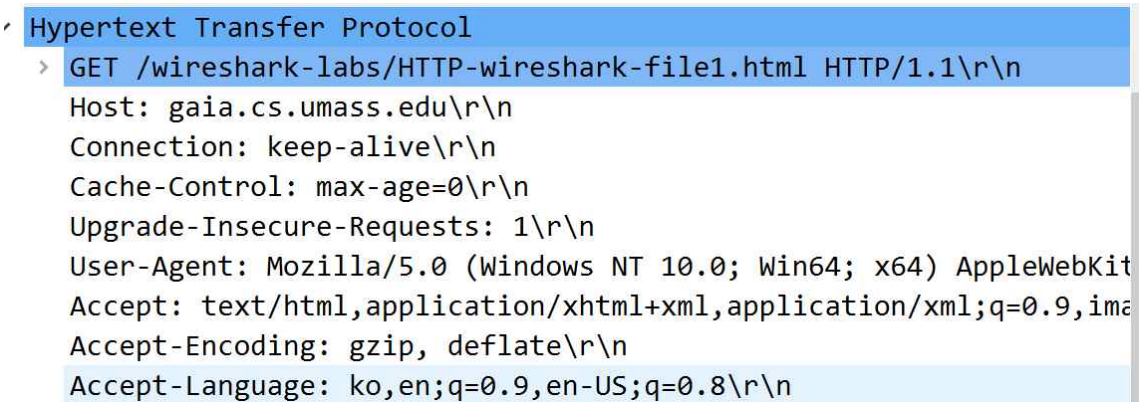
(1)





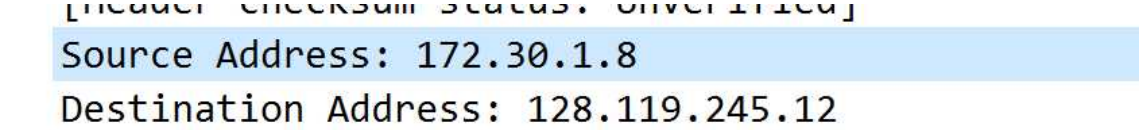
web browser를 키고, http를 display-filter=specification window에 친다. http가 1.1버전인 것을 확인할 수 있다.

(2)



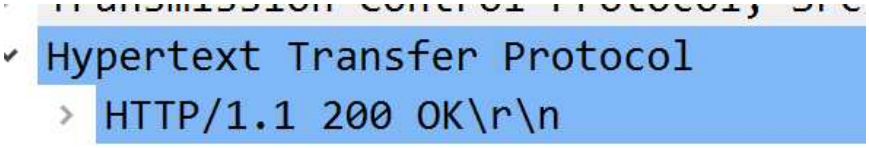
Accept-Language 필드를 보면, ko는 한국어, en은 영어를 나타낸다. q는 품질 인수를 나타내며 0~1까지의 값이 있는데 1에 가까울수록 해당 언어를 선호한다는 뜻이다. en-US는 미국 영어를 나타내는 것으로, 브라우저가 한국어를 가장 선호하고 영어는 일반적인 영어 -> 미국 영어 순서로 선호하는 것을 알 수 있다.

(3)



내 컴퓨터(source)의 IP주소는 172.30.1.8이고, gaia.cs.umass.edu(destination)의 ip주소는 128.30.1.8이다.

(4)

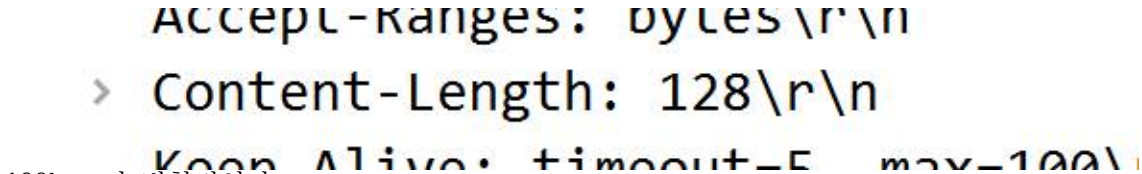


200을 return해줬다. 성공적으로 요청이 처리되었음을 나타낸다.

(5)

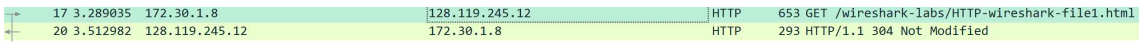
4월 6일 화요일에 마지막으로 수정되었다.

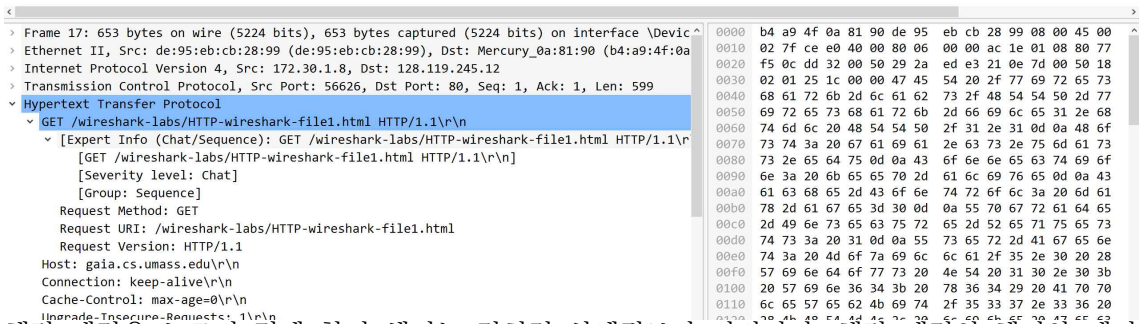
(6)



128byte가 반환되었다.

(7)





해당 패킷을 누르면 밑에 창이 생기는 것처럼 상세정보가 나타난다. 해당 패킷의 헤더와 데이터 등이 16진수와 아스크 코드로 표시되어있다. 패킷 리스트 창에 표시되지 않은 데이터 헤더는 없다.

(8)

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Thu, 06 Apr 2023 11:35:57 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.
  Last-Modified: Thu, 06 Apr 2023 05:59:02 GMT\r\n
  ETag: "173-5f8a49afd5f3f"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.214604000 seconds]
  [Request in frame: 10224]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

보이지 않는다.

(9)

```
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change.  <p>\n
  Thus  if you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

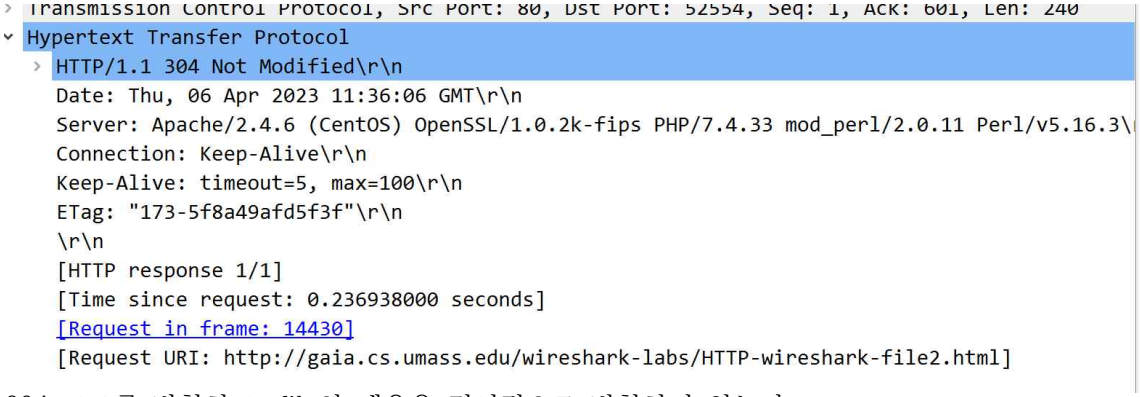
명시적으로 파일 내용을 반환한다.

(10)

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gec
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;c
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
  If-None-Match: "173-5f8a49afd5f3f"\r\n
  If-Modified-Since: Thu, 06 Apr 2023 05:59:02 GMT\r\n
```

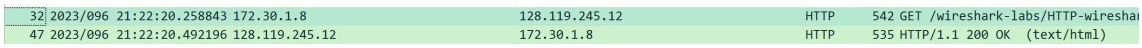
Thu,06 APR 2023 05:59_02 GMT라고 적혀있다. 전에 해당 파일이 수정된 시간이 브라우저에 캐시되어 있는 경우, 서버에서 해당 파일의 수정 시간이 이전과 동일하다면, 서버는 새로운 파일 내용을 반환하지 않고 304 Not Modified 응답을 보내 캐시된 파일을 그대로 사용하도록 한다.

(11)



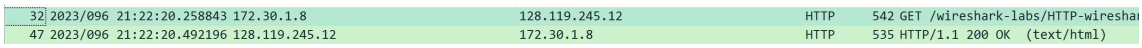
304 코드를 반환하고, file의 내용을 명시적으로 반환하지 않는다.

(12)



한번 보낸다. packet number는 32이다.

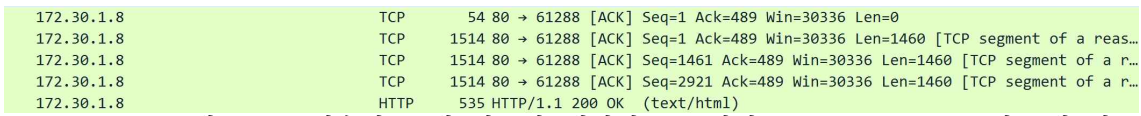
(13,14)



47번 packet number이다.

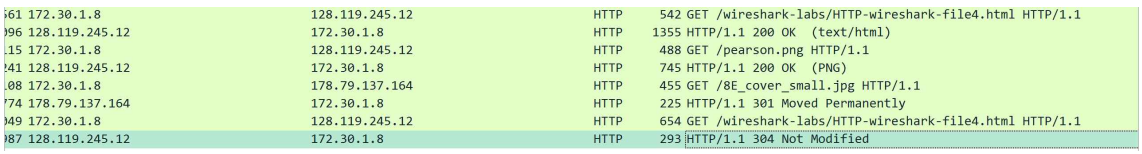
이 패킷의 status code는 200이고, phrase는 OK이다.

(15)



bill of rights 텍스트를 전송하는 데 필요한 데이터를 포함하는 TCP segments가 3개 필요하다. TCP 세그먼트 수는 데이터의 크기 및 TCP 세그먼트 크기에 따라 달라진다.

(16)

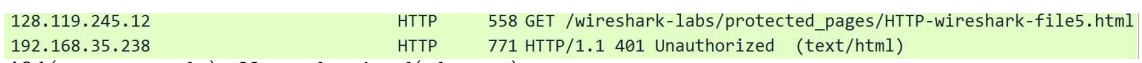


4개, 128.119.245.12/128.119.245.12/178.79.137.164/128.119.245.12

(17)

serially, 차례대로 text/html, png, jpg 파일을 받아온다. jpg파일의 경우 301코드와 함께 클라이언트가 요청한 리소스가 새로운 url로 영구적으로 이동되었음을 나타낸다. 301코드로부터 반환된 리디렉션 웹으로 다시 자동으로 get을 하면 304가 반환이 된다.

(18)



401(status code), Unauthorized(phrase)

(19)

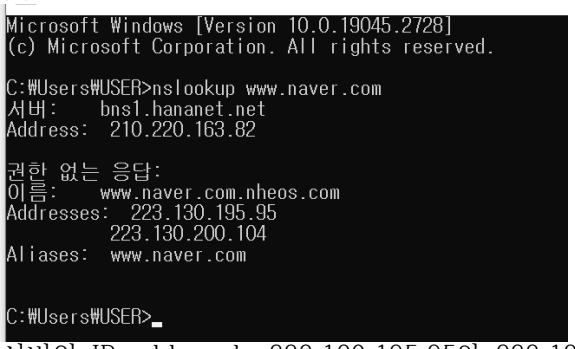
```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
```

위는 두 번째 GET에 생긴 Authorization이라는 헤더이다. 다음 사진은 첫 번째 GET헤더이다. Authoriziation이라는 헤더가 없다. 교재를 보면 위는 id와 password를 인코딩한 것이다.

```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWe
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
\r\n
```

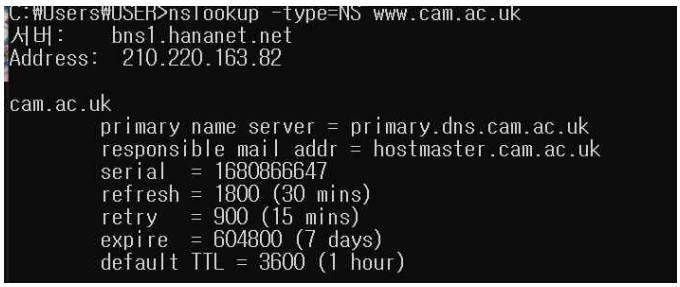
Ⅲ. Question #3

(1)



서버의 IP address는 223.130.195.95와 223.130.200.104이다.

(2)



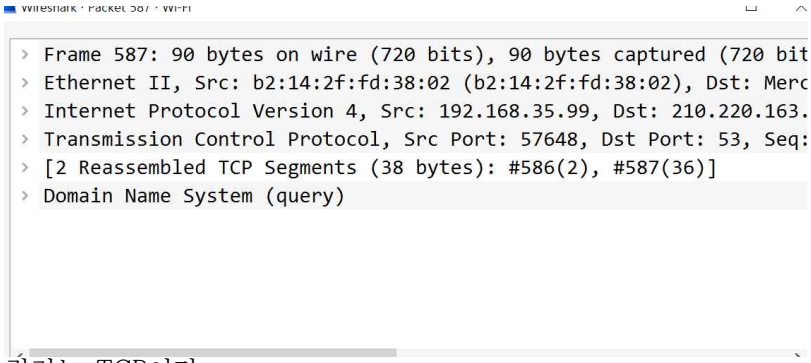
캠브리지대학의 authoritative DNS server는 primary.dns.cam.ac.uk

(3)

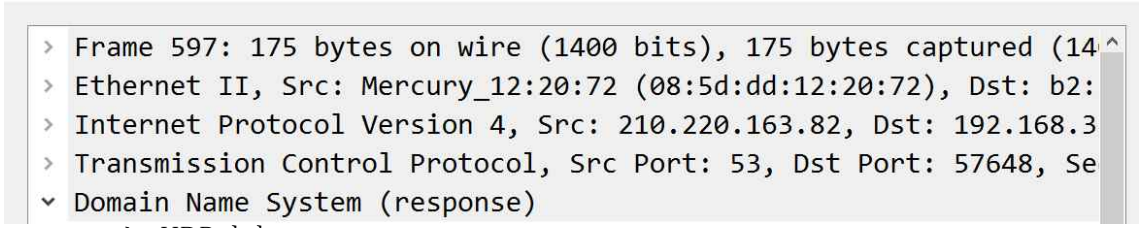
```
C:₩Users₩USER>nslookup primary.dns.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
서버:    UnKnown
Address:  119.161.8.11

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** UnKnown에 대한 요청이 제한 시간을 초과했습니다.
```

캠브리지 DNS server가 야후 메일에 쿼리되었다. 119.161.8.11이라는 ip address를 받아왔다.

(4)

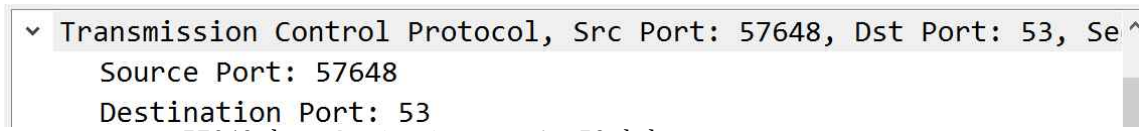


쿼리는 TCP이다.



response는 UDP이다.

(5)



source port: 57648이고, destination port는 53이다.

(6)

```
무선 LAN 어댑터 Wi-Fi:

   연결별 DNS 접미사. . . . :
   설명. . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   물리적 주소 . . . . . . . : B2-14-2F-FD-38-02
   DHCP 사용 . . . . . . . . : 예
   자동 구성 사용. . . . . . : 예
   링크-로컬 IPv6 주소 . . . . : fe80::947e:7ea7:65b2:108f%7(기본 설정)
   IPv4 주소 . . . . . . . . : 192.168.35.99(기본 설정)
   서브넷 마스크 . . . . . . : 255.255.255.0
   임대 시작 날짜. . . . . . : 2023년 4월 7일 금요일 오후 8:14:26
   임대 만료 날짜. . . . . . : 2023년 4월 7일 금요일 오후 9:44:37
   기본 게이트웨이 . . . . . : 192.168.35.1
   DHCP 서버 . . . . . . . . : 192.168.35.1
   DHCPv6 IAID . . . . . . . : 129111087
   DHCPv6 클라이언트 DUID. . : 00-03-00-01-B2-14-2F-FD-38-02
   DNS 서버. . . . . . . . . : 210.220.163.82
                               219.250.36.130
   Tcpip를 통한 NetBIOS. . . . : 사용
```

```
> Internet Protocol Version 4, Src: 192.168.35.99, Dst: 210.220.163.82
```

cmd창에 ipconfig /all 명령어를 치면 내 DNS local server가 210.220.163.82인 것을 확인할 수 있고, 이 주소로 query를 보낸 것을 확인 할 수있다. 즉, 동일하다.

(7)

```
v Domain Name System (query)
    Length: 36
    Transaction ID: 0x818b
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > analytics.ietf.org: type A, class IN
    [Response In: 597]
```

Type A이다. answers란, 해당 도메인 이름에 대한 IP주소가 포함되지만, 없다.

(8)

```
v Domain Name System (response)
    Length: 119
    Transaction ID: 0x818b
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > analytics.ietf.org: type A, class IN
  > Answers
    [Request In: 587]
    [Time: 0.161504000 seconds]
```

3개의 answer가 있다. answer에는 다음과 같이 나타난다.

```
v Answers
  > analytics.ietf.org: type CNAME, class IN, cname analytics.ietf.org.cdn.cloudflare
  > analytics.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
  > analytics.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
  [Request In: 587]
  [Time: 0.161504000 seconds]
```

```
  Name: analytics.ietf.org
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 1800 (30 minutes)
  Data length: 39
  CNAME: analytics.ietf.org.cdn.cloudflare.net
```

웹사이트 이름, 타입, class, TTL, data 길이와 IP address가 있다.

(9)

클라이언트는 서버에게 SYN 패킷을 보내고, 서버는 SYN/ACK패킷을 클라이언트에게 보내고, 클라이언트는 다시 ACK 패킷을 서버에게 보낸다. SYN 패킷 대상 IP주소는 104.16.44.99와 104.16.45.99인데 이 주소를 response ip주소에서도 확인할 수 있다.

(10) 이미지를 검색하기 전엔 새로운 dns가 생성되지 않는다.

(11)

```
Destination Port: 53
```

```
Source Port: 53
```

DNS 쿼리 메시지에서 목적지 포트 넘버는 53이고, response 메시지에서 source 포트 넘버는 53이다.

(12)

```
Internet Protocol Version 4, Src: 192.168.35.99, Dst: 219.250.36.130
```

DNS쿼리 메시지는 내 로컬 dns 서버(219.250.36.130)으로 메시지를 보낸다.

(13)

```
Domain Name System (query)
    Length: 36
    Transaction ID: 0x818b
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > analytics.ietf.org: type A, class IN
    [Response In: 597]
```

A 타입에, answers는 없다.

(14)

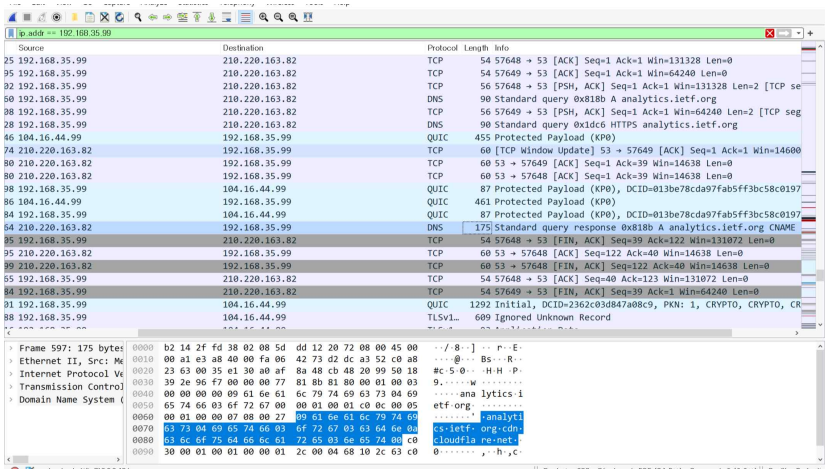
```
Answers
  > analytics.ietf.org: type CNAME, class IN, cname analytics.ietf.org.cdn.cloudflare
  > analytics.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
  > analytics.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
[Request In: 587]
[Time: 0.161504000 seconds]
```

```
Name: analytics.ietf.org
Type: CNAME (Canonical NAME for an alias) (5)
Class: IN (0x0001)
Time to live: 1800 (30 minutes)
Data length: 39
CNAME: analytics.ietf.org.cdn.cloudflare.net
```

웹사이트 이름, 타입, class, TTL, data 길이와 IP address가 있다.

(15)

전체 화면 캡처.



(16)


```
› Internet Protocol Version 4, Src: 192.168.35.99, Dst: 219.250.36.130
```

219.250.36.130 내 local DNS server로 보내고 있다.

(17)

```
  ⌄ Queries
    › www.mit.edu: type A, class IN
    [Response In: 166]
```

type A에 answers는 없다.

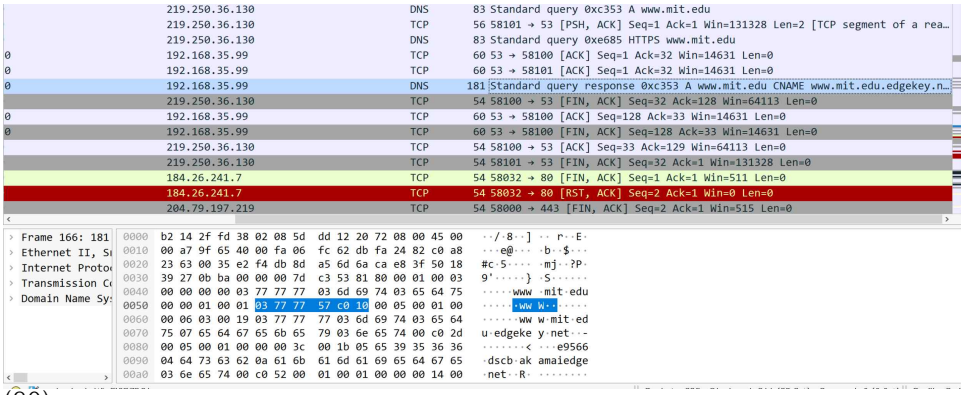
(18)

```
  › Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  › Queries
  ⌄ Answers
    ⌄ wwW.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
        Name: wwW.mit.edu
        Type: CNAME (Canonical NAME for an alias) (5)
        Class: IN (0x0001)
        Time to live: 1539 (25 minutes, 39 seconds)
        Data length: 25
        CNAME: www.mit.edu.edgekey.net
    › www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
```

MIT nameservers는 www.mit.edu와 www.mit.edu.edgekey.net을 제공한다. IP address가 포함되어있지않다.

(19)

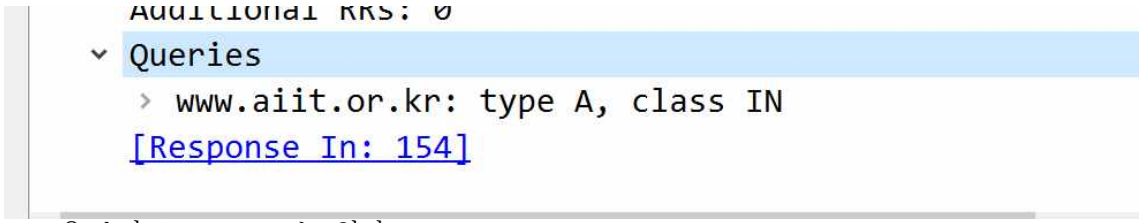
전체 화면 캡처



(20)

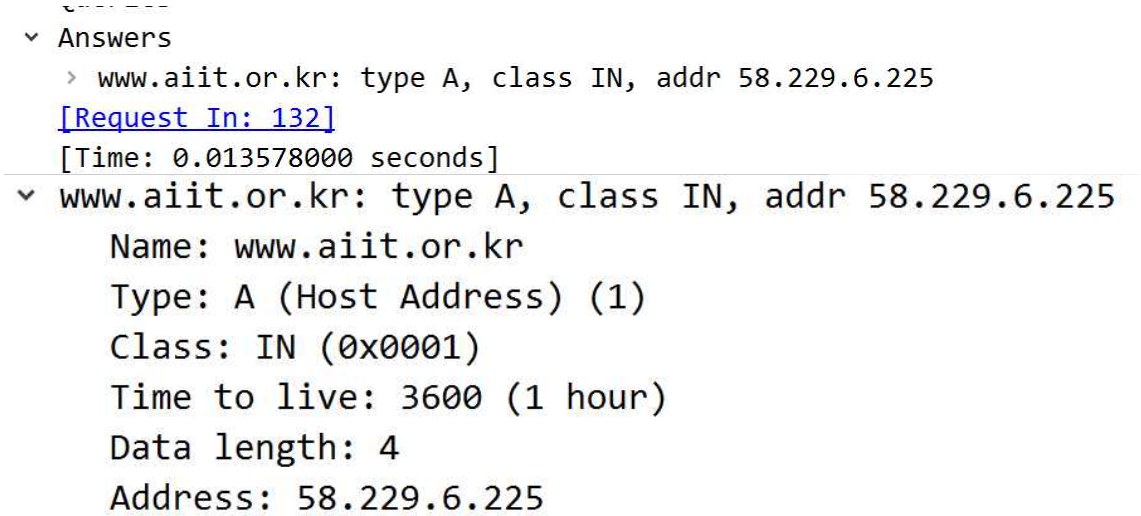
내 local dns서버로 보내고 있다.

(21)



type은 A이고, answers는 없다.

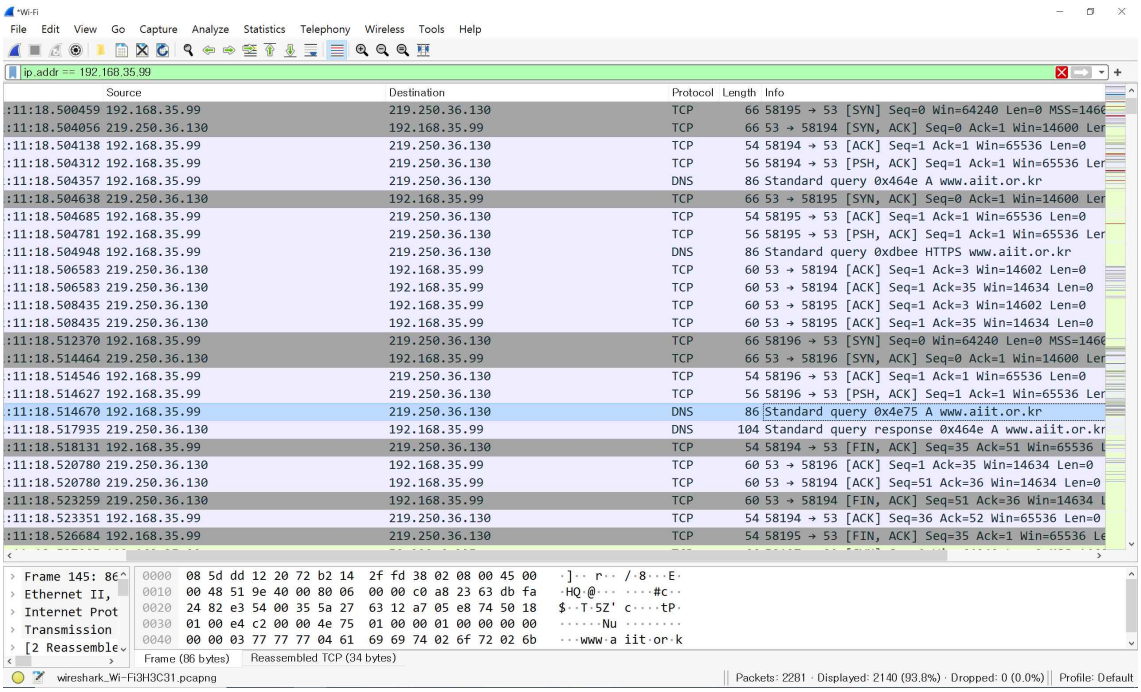
(22)



하나의 answers를 가지며, 타입, class, 웹사이트 이름, 주소를 가진다.

(23)

전체화면캡처. 전체적인 흐름을 파악할 수 있다.



Ⅳ. 고찰

네트워크라는 과목도 처음이고, wireshark도 처음이라 맨 처음에 적응하는 데에 시간이 많이 걸렸다. 또한, 교재에 나온 것처럼 GET에 대한 response가 바로 다음 줄에 나타나지 않고, 사이 사이에 다른 http packet들이 섞여 있어 맞는 GET에 대한 response를 찾아야했다. DNS의 경우 cmd창을 이용해 내 local dns address로 query가 보내진다는 점이 흥미로웠다. 또한 http의 경우 수업 시간에 배운 것처럼 object들을 한 번에 가져오는 것이 아니라 한 번에 한번씩 여러번 왔다 갔다하는 것을 직접 실습을 통해 보게 되어 신기했다.