

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>ipconfig

Windows IP 구성

무선 LAN 어댑터 로컬 영역 연결* 1:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . . :

무선 LAN 어댑터 로컬 영역 연결* 10:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . . :

이더넷 어댑터 이더넷 2:

    연결별 DNS 접미사. . . . :
    링크-로컬 IPv6 주소 . . . : fe80::f389:e520:20ec:b566%23
    IPv4 주소 . . . . . : 192.168.92.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

이더넷 어댑터 이더넷 3:

    연결별 DNS 접미사. . . . :
    링크-로컬 IPv6 주소 . . . : fe80::200:9143:a3b4:4708%3
    IPv4 주소 . . . . . : 192.168.112.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

무선 LAN 어댑터 Wi-Fi:

    연결별 DNS 접미사. . . . :
    IPv6 주소 . . . . . : 2001:2d8:6a2b:db24:72c5:4b73:4d0a:b675
    임시 IPv6 주소 . . . . . : 2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418
    링크-로컬 IPv6 주소 . . . : fe80::88ce:62cd:1727:660c%7
    IPv4 주소 . . . . . : 192.168.190.224
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : fe80::74bb:b9ff:fe69:8d02%7
    192.168.190.162

이더넷 어댑터 Bluetooth 네트워크 연결:

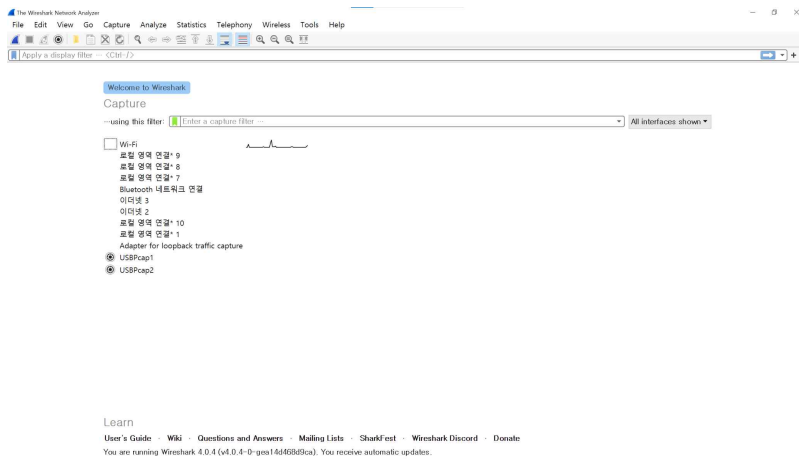
    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사. . . . :

C:\Users\USER>
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Mercury_0a:81:90	Broadcast	ARP	42	Who's on the network?
2	0.333917	Mercury_0a:81:90	Broadcast	ARP	42	Who's on the network?
3	0.513312	172.30.1.48	224.0.0.251	MDNS	330	Stale
4	0.514270	fe80::898:b829:f3d4:d20e	ff02::fb	MDNS	350	Stale
5	0.514270	172.30.1.48	224.0.0.251	MDNS	198	Stale
6	0.514270	fe80::898:b829:f3d4:d20e	ff02::fb	MDNS	218	Stale
7	0.764638	172.30.1.48	224.0.0.251	MDNS	233	Stale
8	0.764638	fe80::898:b829:f3d4:d20e	ff02::fb	MDNS	253	Stale
9	1.017064	172.30.1.48	224.0.0.251	MDNS	233	Stale
10	1.017469	fe80::898:b829:f3d4:d20e	ff02::fb	MDNS	253	Stale
11	1.263476	Mercury_0a:81:90	Broadcast	ARP	42	Who's on the network?
12	1.267169	172.30.1.48	224.0.0.251	MDNS	655	Stale
13	1.267169	fe80::898:b829:f3d4:d20e	ff02::fb	MDNS	675	Stale

II. Question #2

(1)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.190.224	211.115.106.202	HTTP	443	GET /jk?c=62&p=3nQyHT1X4cUdy1_t0fY7Qa4LFRzrX2v
2	0.000000	192.168.190.224	211.115.106.202	HTTP	443	GET /jk?c=62&p=3nQyHT1X4cUdy1_t0fY7Qa4LFRzrX2v
3	0.000000	211.115.106.202	192.168.190.224	HTTP	415	HTTP/1.1 200 OK
4	0.000000	211.115.106.202	192.168.190.224	HTTP	415	HTTP/1.1 200 OK
5	0.000000	2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418	2600:1410:c000::addf:e308	HTTP	466	GET /roots/dstrootcax3.p7c HTTP/1.1
6	0.000000	2600:1410:c000::addf:e308	2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418	HTTP	344	HTTP/1.1 304 Not Modified
7	0.000000	2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418	2600:1410:2000:1a4::21cc	HTTP	436	GET / HTTP/1.1
8	0.000000	2600:1410:2000:1a4::21cc	2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418	HTTP	339	HTTP/1.1 304 Not Modified
9	0.000000	2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418	2600:1410:2000:1bd::21cc	HTTP	436	GET / HTTP/1.1
10	0.000000	2600:1410:2000:1bd::21cc	2001:2d8:6a2b:db24:c5ec:6ffb:926c:3418	HTTP	338	HTTP/1.1 304 Not Modified

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

(2)

• Hypertext Transfer Protocol

```

> GET /wireshark-labs/HTTP-wireshark-file1.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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n

```

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)

[Product Checksum Status: OK]

Source Address: 172.30.1.8

Destination Address: 128.119.245.12

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

(4)

```

Transmission Control Protocol, Src
✓ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n

```

200을 return해줬다. 성공적으로 요청이 처리되었음을 나타낸다.

(5)

```

Last-Modified: Thu, 06 Apr 2023 05:59:02 GMT\r\n

```

4월 6일 화요일에 마지막으로 수정되었다.

(6)

```

Accept-Ranges: bytes\r\n
> Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n

```

128byte가 반환되었다.

(7)

17	3.289035	172.30.1.8	128.119.245.12	HTTP	653 GET /wireshark-labs/HTTP-wireshark-file1.html
20	3.512982	128.119.245.12	172.30.1.8	HTTP	293 HTTP/1.1 304 Not Modified

```

<
> Frame 17: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \Device
> Ethernet II, Src: de:95:eb:cb:28:99 (de:95:eb:cb:28:99), Dst: Mercury_0a:81:90 (b4:a9:4f:0a
> Internet Protocol Version 4, Src: 172.30.1.8, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 56626, Dst Port: 80, Seq: 1, Ack: 1, Len: 599
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
      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
      0000 b4 a9 4f 0a 81 90 de 95 eb cb 28 99 08 00 45 00
      0010 02 7f ce e0 40 00 80 06 00 00 ac 1e 01 08 80 77
      0020 f5 0c dd 32 00 50 29 2a ed e3 21 0e 7d 00 50 18
      0030 02 01 25 1c 00 00 47 45 54 20 2f 77 69 72 65 73
      0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
      0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
      0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
      0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
      0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f
      0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43
      00a0 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61
      00b0 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 64 65
      00c0 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73
      00d0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e
      00e0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
      00f0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b
      0100 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70
      0110 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20

```

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

(8)

```

v 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
v 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)

```

v 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 Ge
    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)

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 52554, Seq: 1, ACK: 601, Len: 240
  ▾ Hypertext Transfer Protocol
    > HTTP/1.1 304 Not Modified\r\n
      Date: Thu, 06 Apr 2023 11:36:06 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Connection: Keep-Alive\r\n
      Keep-Alive: timeout=5, max=100\r\n
      ETag: "173-5f8a49afd5f3f"\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.236938000 seconds]
      [Request in frame: 14430]
      [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

304 코드를 반환하고, file의 내용을 명시적으로 반환하지 않는다.

(12)

32	2023/096	21:22:20.258843	172.30.1.8	128.119.245.12	HTTP	542 GET /wireshark-labs/HTTP-wireshark-file2.html
47	2023/096	21:22:20.492196	128.119.245.12	172.30.1.8	HTTP	535 HTTP/1.1 200 OK (text/html)

한번 보낸다. packet number는 32이다.

(13,14)

32	2023/096	21:22:20.258843	172.30.1.8	128.119.245.12	HTTP	542 GET /wireshark-labs/HTTP-wireshark-file2.html
47	2023/096	21:22:20.492196	128.119.245.12	172.30.1.8	HTTP	535 HTTP/1.1 200 OK (text/html)

47번 packet number이다.

이 패킷의 status code는 200이고, phrase는 OK이다.

(15)

172.30.1.8	TCP	54 80 → 61288 [ACK] Seq=1 Ack=489 Win=30336 Len=0
172.30.1.8	TCP	1514 80 → 61288 [ACK] Seq=1 Ack=489 Win=30336 Len=1460 [TCP segment of a reassembled data segment]
172.30.1.8	TCP	1514 80 → 61288 [ACK] Seq=1461 Ack=489 Win=30336 Len=1460 [TCP segment of a reassembled data segment]
172.30.1.8	TCP	1514 80 → 61288 [ACK] Seq=2921 Ack=489 Win=30336 Len=1460 [TCP segment of a reassembled data segment]
172.30.1.8	HTTP	535 HTTP/1.1 200 OK (text/html)

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)

161	172.30.1.8	128.119.245.12	HTTP	542 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
196	128.119.245.12	172.30.1.8	HTTP	1355 HTTP/1.1 200 OK (text/html)
115	172.30.1.8	128.119.245.12	HTTP	488 GET /pearson.png HTTP/1.1
141	128.119.245.12	172.30.1.8	HTTP	745 HTTP/1.1 200 OK (PNG)
108	172.30.1.8	178.79.137.164	HTTP	455 GET /8E_cover_small.jpg HTTP/1.1
174	178.79.137.164	172.30.1.8	HTTP	225 HTTP/1.1 301 Moved Permanently
149	172.30.1.8	128.119.245.12	HTTP	654 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
187	128.119.245.12	172.30.1.8	HTTP	293 HTTP/1.1 304 Not Modified

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)

128.119.245.12	HTTP	558 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
192.168.35.238	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)

401(status code), Unauthorized(phrase)

(19)

```
Cache-Control: max-age=0\r\n
```

> Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=\r\n

위는 두 번째 GET에 생긴 Authorization이라는 헤더이다. 다음 사진은 첫 번째 GET헤더이다. Authorization이라는 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) AppleWebKit

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)

```
Microsoft Windows [Version 10.0.19045.2728]  
(c) Microsoft Corporation. All rights reserved.
```

```
C:\Users\WUSER>nslookup www.naver.com
```

```
서버: bns1.hananet.net
```

```
Address: 210.220.163.82
```

```
권한 없는 응답:
```

```
이름: www.naver.com.nheos.com
```

```
Addresses: 223.130.195.95
```

```
223.130.200.104
```

```
Aliases: www.naver.com
```

```
C:\Users\WUSER>
```

서버의 IP address는 223.130.195.95와 223.130.200.104이다.

(2)

```
C:\Users\WUSER>nslookup -type=NS www.cam.ac.uk
```

```
서버: bns1.hananet.net
```

```
Address: 210.220.163.82
```

```
cam.ac.uk
```

```
primary name server = primary.dns.cam.ac.uk
```

```
responsible mail addr = hostmaster.cam.ac.uk
```

```
serial = 1680866647
```

```
refresh = 1800 (30 mins)
```

```
retry = 900 (15 mins)
```

```
expire = 604800 (7 days)
```

```
default TTL = 3600 (1 hour)
```

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)

```

Wireshark - Packet 507 - Wi-Fi
> Frame 587: 90 bytes on wire (720 bits), 90 bytes captured (720 bit
> Ethernet II, Src: b2:14:2f:fd:38:02 (b2:14:2f:fd:38:02), Dst: Merc
> Internet Protocol Version 4, Src: 192.168.35.99, Dst: 210.220.163.
> Transmission Control Protocol, Src Port: 57648, Dst Port: 53, Seq:
> [2 Reassembled TCP Segments (38 bytes): #586(2), #587(36)]
> Domain Name System (query)

```

쿼리는 TCP이다.

```

> Frame 597: 175 bytes on wire (1400 bits), 175 bytes captured (14
> Ethernet II, Src: Mercury_12:20:72 (08:5d:dd:12:20:72), Dst: b2:
> Internet Protocol Version 4, Src: 210.220.163.82, Dst: 192.168.3
> Transmission Control Protocol, Src Port: 53, Dst Port: 57648, Se
> Domain Name System (response)

```

response는 UDP이다.

(5)

```

Transmission Control Protocol, Src Port: 57648, Dst Port: 53, Seq
Source Port: 57648
Destination Port: 53

```

source port: 57648이고, destination port는 53이다.

(6)

```

무선 LAN 어댑터 Wi-Fi:
연결된 DNS 접미사. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
물리적 주소. . . . . : B2-14-2F-FD-38-02
DHCP 사용. . . . . : 예
자동 구성 사용. . . . . : 예
링크로 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)

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

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

(8)

```
▼ 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
  ▼ Queries
    > analytics.ietf.org: type A, class IN
  > Answers
    [Request In: 587]
    [Time: 0.161504000 seconds]
```

3개의 answer가 있다. answer에는 다음과 같이 나타난다.

```
▼ 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 번호는 53이고, response 메시지에서 source 포트 번호는 53이다.

(12)

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

DNS 서버 : 210.220.163.82
219.250.36.130

Tcpip를 통한 NetBIOS : 사용

DNS 쿼리 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
▼ 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.

Source	Destination	Protocol	Length	Info
25 192.168.35.99	210.220.163.82	TCP	54	57648 → 53 [ACK] Seq=1 Ack=1 Win=131328 Len=0
95 192.168.35.99	210.220.163.82	TCP	54	57649 → 53 [ACK] Seq=1 Ack=1 Win=64240 Len=0
82 192.168.35.99	210.220.163.82	TCP	56	57648 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP se
50 192.168.35.99	210.220.163.82	DNS	90	Standard query 0x818b A analytics.ietf.org
88 192.168.35.99	210.220.163.82	TCP	56	57649 → 53 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=2 [TCP seg
28 192.168.35.99	210.220.163.82	DNS	90	Standard query 0x1dc6 HTTPS analytics.ietf.org
46 104.16.44.99	192.168.35.99	QUIC	455	Protected Payload (KPB)
74 210.220.163.82	192.168.35.99	TCP	60	[TCP Window Update] 53 → 57649 [ACK] Seq=1 Ack=1 Win=14600
80 210.220.163.82	192.168.35.99	TCP	60	53 → 57649 [ACK] Seq=1 Ack=39 Win=14638 Len=0
80 210.220.163.82	192.168.35.99	TCP	60	53 → 57648 [ACK] Seq=1 Ack=39 Win=14638 Len=0
98 192.168.35.99	104.16.44.99	QUIC	87	Protected Payload (KPB), DCID=013be78cda97fab5ff3bc58c0197
86 104.16.44.99	192.168.35.99	QUIC	461	Protected Payload (KPB)
84 192.168.35.99	104.16.44.99	QUIC	87	Protected Payload (KPB), DCID=013be78cda97fab5ff3bc58c0197
54 210.220.163.82	192.168.35.99	DNS	175	Standard query response 0x818b A analytics.ietf.org CNAME
95 192.168.35.99	210.220.163.82	TCP	54	57648 → 53 [FIN, ACK] Seq=39 Ack=122 Win=131072 Len=0
95 210.220.163.82	192.168.35.99	TCP	60	53 → 57648 [ACK] Seq=122 Ack=40 Win=14638 Len=0
99 210.220.163.82	192.168.35.99	TCP	60	53 → 57648 [FIN, ACK] Seq=122 Ack=40 Win=14638 Len=0
95 192.168.35.99	210.220.163.82	TCP	54	57648 → 53 [ACK] Seq=40 Ack=123 Win=131072 Len=0
84 192.168.35.99	210.220.163.82	TCP	54	57649 → 53 [FIN, ACK] Seq=39 Ack=1 Win=64240 Len=0
81 192.168.35.99	104.16.44.99	QUIC	1292	Initial, DCID=2362c03d847a08c9, PKN: 1, CRYPTO, CRYPTO, CR
88 192.168.35.99	104.16.44.99	TLSv1.	609	Ignored Unknown Record

(16)

```
DHCPv6 클라이언트 DUID. . . : 00-03-00-01-B2-14-7
DNS 서버. . . . . : 210.220.163.82
                  219.250.36.130
Tcpip를 통한 NetBIOS . . . : 사용
```

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

219.250.36.130	DNS	83 Standard query 0xc353 A www.mit.edu
219.250.36.130	TCP	56 58101 → 53 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=2 [TCP segment of a rea..
219.250.36.130	DNS	83 Standard query 0xc685 HTTPS www.mit.edu
0	TCP	60 53 → 58100 [ACK] Seq=1 Ack=32 Win=14631 Len=0
0	TCP	60 53 → 58101 [ACK] Seq=1 Ack=32 Win=14631 Len=0
0	DNS	181 Standard query response 0xc353 A www.mit.edu CNAME www.mit.edu.edgekey.n...
219.250.36.130	TCP	54 58100 → 53 [FIN, ACK] Seq=32 Ack=128 Win=64113 Len=0
0	TCP	60 53 → 58100 [ACK] Seq=128 Ack=33 Win=14631 Len=0
0	TCP	60 53 → 58100 [FIN, ACK] Seq=128 Ack=33 Win=14631 Len=0
0	TCP	54 58100 → 53 [ACK] Seq=33 Ack=129 Win=64113 Len=0
219.250.36.130	TCP	54 58101 → 53 [FIN, ACK] Seq=32 Ack=1 Win=131328 Len=0
184.26.241.7	TCP	54 58032 → 80 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0
184.26.241.7	TCP	54 58032 → 80 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
204.79.197.219	TCP	54 58000 → 443 [FIN, ACK] Seq=2 Ack=1 Win=515 Len=0

> Frame 166: 181	0000	b2 14 2f fd 38 02 08 5d dd 12 20 72 08 00 45 00	..-/8-..] .. n..E
> Ethernet II, Si	0010	00 a7 9f 65 40 00 fa 06 fc 62 db fa 24 82 c0 a8	..e@... ..b-\$...
> Internet Proto	0020	23 63 00 35 e2 f4 db 8d a5 6d 6a ca e8 3f 50 18	#c 5... ..mj...?p
> Transmission C	0030	39 27 0b ba 00 00 00 7d c3 53 81 80 00 01 00 03	9'.....} S'.....
> Domain Name Sy	0040	00 00 00 00 03 77 77 77 03 6d 69 74 03 65 64 75www..mit..edu
	0050	00 00 01 00 01 03 77 77 57 c0 10 00 05 00 01 00www..w...net...
	0060	00 06 03 00 19 03 77 77 77 03 6d 69 74 03 65 64www..mit..ed
	0070	75 07 65 64 67 65 6b 65 79 03 6e 65 74 00 c0 2d	u..edgekey..net...
	0080	00 05 00 01 00 00 00 3c 00 1b 05 65 39 35 36 36<.....e9566
	0090	04 64 73 63 62 0a 61 6b 61 6d 61 69 65 64 67 65	..dsdb..ak..amaledge
	00a0	03 6e 65 74 00 c0 52 00 01 00 01 00 00 00 14 00	..net..R.....

(20)

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

DNS 서버 : 210.220.163.82
219.250.36.130
Tcpip를 통한 NetBIOS : 사용

내 local dns서버로 보내고 있다.

(21)

ADDITIONAL RRS: 0
▼ Queries
> www.aiit.or.kr: type A, class IN
[\[Response In: 154\]](#)

type은 A이고, answers는 없다.

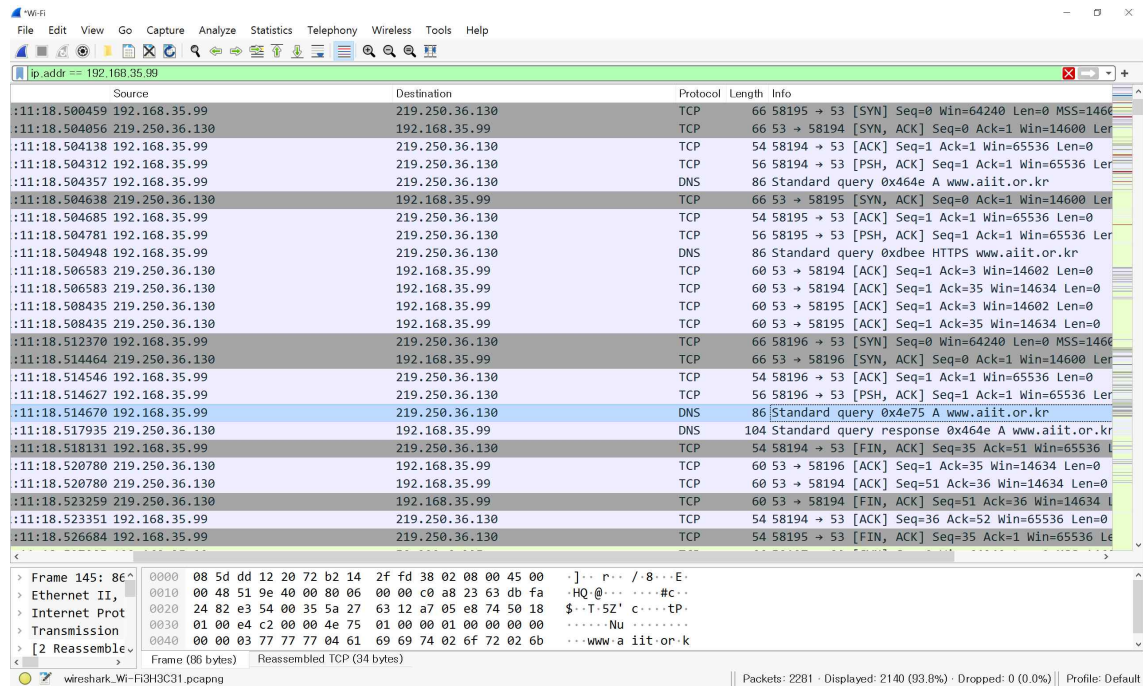
(22)

▼ Answers
> www.aiit.or.kr: type A, class IN, addr 58.229.6.225
[\[Request In: 132\]](#)
[Time: 0.013578000 seconds]
▼ www.aiit.or.kr: type A, class IN, addr 58.229.6.225
Name: www.aiit.or.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 4
Address: 58.229.6.225

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.