

컴퓨터네트워크 Wireshark 과제

교수님 성함: 이혁준 교수

강의 명: 컴퓨터네트워크

강의 시간: 월 4교시, 수 3교시

소속: 컴퓨터정보공학부

학번: 2018202074

이름: 김상우

제출일: 2022.04.13

서론

위 과제는 Wireshark의 기본적인 사용법과 사용 목적을 이해하고 해당 응용프로그램을 실무에서 사용할 수 있는 실력을 얻는 것을 목적으로 두고 있다. 이 과정에서 Wireshark의 본 목적이 네트워크의 흐름을 파악하는 것에 있는 만큼 네트워크가 어떻게 작동하는 지를 파악할 수 있으며 그 과정에서 IP, TCP, Http등 다양한 네트워크 구성 요소들을 직, 간접적으로 경험하며 지금까지 배운 컴퓨터 네트워크의 기본적인 내용들을 복습하며 동시에 알아가는 것을 부가적인 목표로 하고 있다.

우리는 이 과제에서 Wireshark를 이용한 Http, DNS 측정과 분석을 하게 될 것이다. 또한 질문에 대한 답변을 스스로 탐색하는 것이 주된 과정이라고 할 수 있다.

본문

Question #1

다음은 cmd에서 ipconfig를 입력해 ip 화면을 캡처한 모습이다. 아래와 같이 Ipconfig는 DNS 서버주소, 주소, 어댑터 타입을 포함하는 현재의 TCP/IP 정보를 보여주고 있음을 알 수 있다.

```
C:\Users\KimSangWoo>ipconfig

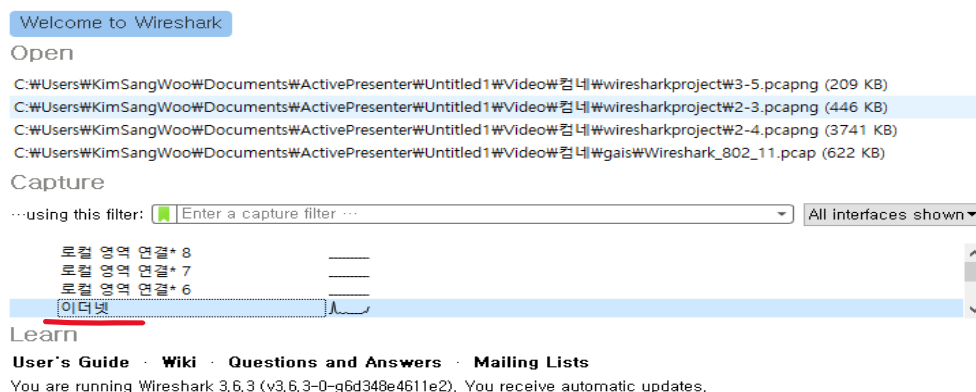
Windows IP 구성

이더넷 어댑터 이더넷:

    연결별 DNS 접미사 . . . . . :
    링크-로컬 IPv6 주소 . . . . . : fe80::4883:7607:d6f4:c556%11
    IPv4 주소 . . . . . : 172.16.103.29
    서브넷 마스크 . . . . . : 255.255.252.0
    기본 게이트웨이 . . . . . : 172.16.103.254

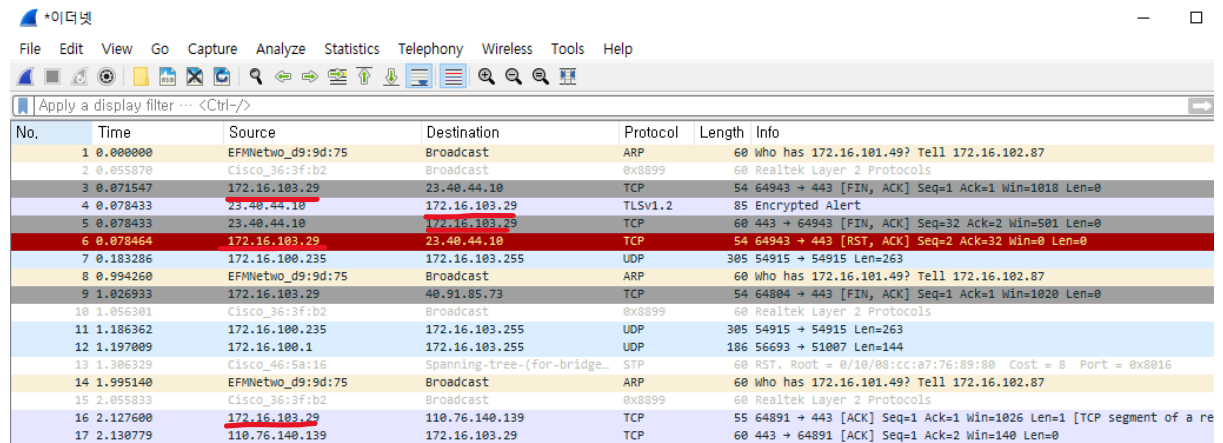
C:\Users\KimSangWoo>
```

이후 Wireshark를 실행, 이더넷을 통해 Wireshark를 분석하기로 했다.

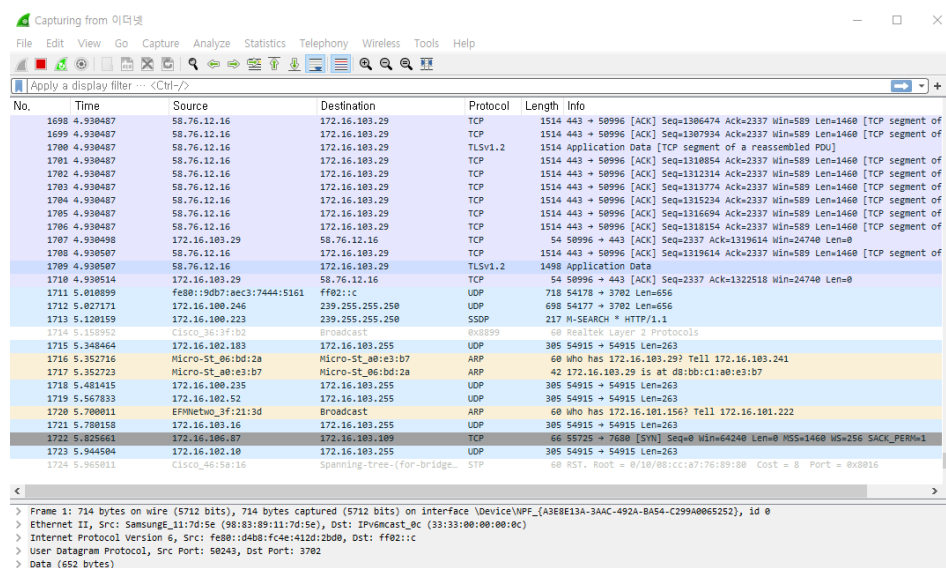


PC에서 동작중인 Wireshark화면을 캡처할 경우 다음과 같이 표시된다.

아래화면의 Source를 확인해보면 config에서 출력된 IPv4주소인 172.16.103.29를 Source하는 경우가 다수 존재함을 확인할 수 있다.

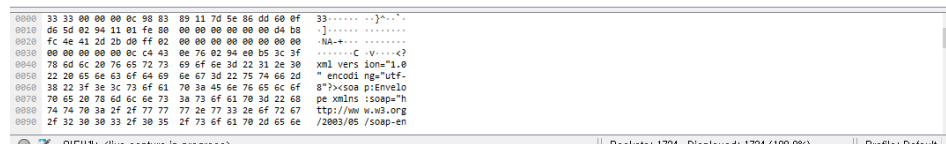


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	EFMNetwo_d9:9d:75	Broadcast	ARP	60	who has 172.16.101.49? Tell 172.16.102.87
2	0.055870	Cisco_36:3f:b2	Broadcast	0x8899	60	Realtek Layer 2 Protocols
3	0.071547	172.16.103.29	23.40.44.10	TCP	54	64943 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1018 Len=0
4	0.078433	23.40.44.10	172.16.103.29	TLSv1.2	85	Encrypted Alert
5	0.078433	23.40.44.10	172.16.103.29	TCP	60	443 → 64943 [FIN, ACK] Seq=32 Ack=2 Win=501 Len=0
6	0.078464	172.16.103.29	23.40.44.10	TCP	54	64943 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
7	0.183286	172.16.100.235	172.16.103.255	UDP	305	54915 → 54915 Len=263
8	0.994260	EFMNetwo_d9:9d:75	Broadcast	ARP	60	who has 172.16.101.49? Tell 172.16.102.87
9	1.026933	172.16.103.29	40.91.85.73	TCP	54	64804 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1020 Len=0
10	1.056301	Cisco_36:3f:b2	Broadcast	0x8899	60	Realtek Layer 2 Protocols
11	1.186362	172.16.100.235	172.16.103.255	UDP	305	54915 → 54915 Len=263
12	1.197009	172.16.100.1	172.16.103.255	UDP	186	56693 → 51007 Len=144
13	1.306329	Cisco_46:58:16	Spanning-tree-(for-bridge_	STP	60	RST. Root = 0/10/08:cc:a7:76:89:80 Cost = 8 Port = 0x8016
14	1.995140	EFMNetwo_d9:9d:75	Broadcast	ARP	60	who has 172.16.101.49? Tell 172.16.102.87
15	2.055833	Cisco_36:3f:b2	Broadcast	0x8899	60	Realtek Layer 2 Protocols
16	2.127600	172.16.103.29	110.76.140.139	TCP	55	64891 → 443 [ACK] Seq=1 Ack=1 Win=1026 Len=1 [TCP segment of a re
17	2.130779	110.76.140.139	172.16.103.29	TCP	60	443 → 64891 [ACK] Seq=1 Ack=2 Win=140 Len=0



No.	Time	Source	Destination	Protocol	Length	Info
1698	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1306474 Ack=2337 Win=589 Len=1460 [TCP segment of
1699	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1307934 Ack=2337 Win=589 Len=1460 [TCP segment of
1700	4.930487	58.76.12.16	172.16.103.29	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
1701	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1310854 Ack=2337 Win=589 Len=1460 [TCP segment of
1702	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1313214 Ack=2337 Win=589 Len=1460 [TCP segment of
1703	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1313774 Ack=2337 Win=589 Len=1460 [TCP segment of
1704	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1315234 Ack=2337 Win=589 Len=1460 [TCP segment of
1705	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1316094 Ack=2337 Win=589 Len=1460 [TCP segment of
1706	4.930487	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1318154 Ack=2337 Win=589 Len=1460 [TCP segment of
1707	4.930487	172.16.103.29	58.76.12.16	TCP	54	50996 → 443 [ACK] Seq=2337 Ack=1319614 Win=24740 Len=0
1708	4.930507	58.76.12.16	172.16.103.29	TCP	1514	443 → 50996 [ACK] Seq=1319614 Ack=2337 Win=589 Len=1460 [TCP segment of
1709	4.930507	58.76.12.16	172.16.103.29	TLSv1.2	1498	Application Data
1710	4.930514	172.16.103.29	58.76.12.16	TCP	54	50996 → 443 [ACK] Seq=2337 Ack=1322518 Win=24740 Len=0
1711	5.010899	fe80::9db7:ae33:7444:5161	ff02::c	UDP	718	54178 → 3702 Len=656
1712	5.027171	172.16.100.246	239.255.255.250	UDP	698	54177 → 3702 Len=656
1713	5.120159	172.16.100.223	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
1714	5.120162	Cisco_36:3f:b2	Broadcast	0x8899	60	Realtek Layer 2 Protocols
1715	5.348464	172.16.102.183	172.16.103.255	UDP	305	54915 → 54915 Len=263
1716	5.352716	Micro-St_06:bd:2a	Micro-St_06:bd:2a	ARP	60	who has 172.16.103.29? Tell 172.16.103.241
1717	5.352723	Micro-St_06:bd:2a	Micro-St_06:bd:2a	ARP	42	172.16.103.29 is at d8:bb:c1:a0:e3:b7
1718	5.481415	172.16.100.235	172.16.103.255	UDP	305	54915 → 54915 Len=263
1719	5.567833	172.16.102.52	172.16.103.255	UDP	305	54915 → 54915 Len=263
1720	5.700011	EFMNetwo_3f:21:3d	Broadcast	ARP	60	who has 172.16.101.156? Tell 172.16.101.222
1721	5.780158	172.16.103.16	172.16.103.255	UDP	305	54915 → 54915 Len=263
1722	5.825661	172.16.106.87	172.16.103.109	TCP	66	55725 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1723	5.944584	172.16.102.10	172.16.103.255	UDP	305	54915 → 54915 Len=263
1724	5.965811	Cisco_46:58:16	Spanning-tree-(for-bridge_	STP	60	RST. Root = 0/10/08:cc:a7:76:89:80 Cost = 8 Port = 0x8016

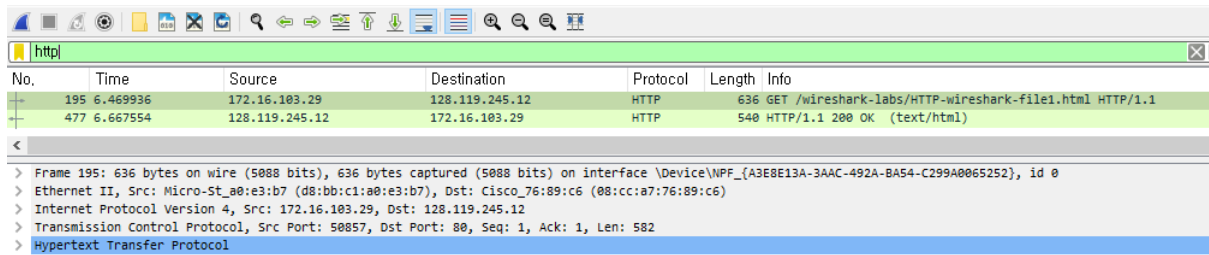
> Frame 1: 714 bytes on wire (5712 bits), 714 bytes captured (5712 bits) on interface \Device\NPF_{A3EBE13A-3A4C-492A-B454-C299A0065252}, id 0
> Ethernet II, Src: Samsung11:70:5e (98:8b:89:11:70:5e), Dst: IPv6multicast (33:33:00:00:00:00)
> Internet Protocol Version 6, Src: fe80::d4b8:fc4e:412d:2d08, Dst: ff02::c
> User Datagram Protocol, Src Port: 50243, Dst Port: 3702
> Data (652 bytes)



0000	33 33 00 00 00 00 0c 98 83 89 11 7d 5e 86 dd 60 bf	33----->
0010	06 5d 02 94 11 01 fe 00 00 00 00 00 04 b8	----->
0020	fc 4e 41 2d 2b d0 ff 02 00 00 00 00 00 00 00	----->
0030	00 00 00 00 00 00 c4 43 0e 76 02 94 e0 b5 3c 3f	----->
0040	70 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30	----->
0050	22 20 65 66 63 6f 64 69 6e 67 3d 22 75 74 66 2d	----->
0060	38 22 3f 3e 3c 73 6f 61 70 3a 45 6e 76 65 6c 6f	----->
0070	70 65 20 78 6d 6c 66 73 30 73 6f 61 70 3d 22 68	----->
0080	74 74 70 3a 2f 2f 77 77 2e 77 33 2e 6f 72 6f	----->
0090	2f 32 30 30 3c 2f 30 35 2f 73 6f 61 70 2d 65 6e	----->

(PC에서 동작중인 WireShark의 화면 모습이다.)

Question #2 (Wireshark_HTTP_v7.0.pdf의 19개 문제 풀이)



No.	Time	Source	Destination	Protocol	Length	Info
195	6.469936	172.16.103.29	128.119.245.12	HTTP	636	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
477	6.667554	128.119.245.12	172.16.103.29	HTTP	540	HTTP/1.1 200 OK (text/html)

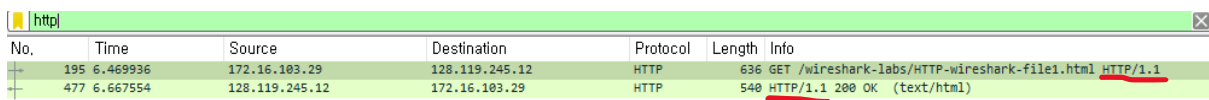
> Frame 195: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50857, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
> Hypertext Transfer Protocol

다음은 <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>로 들어간 후 Wireshark를 통해 확인한 http에 관한 정보만을 display한 결과이다. 이를 바탕으로 질문1~7을 분석한다.

Congratulations. You've downloaded the file <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>!

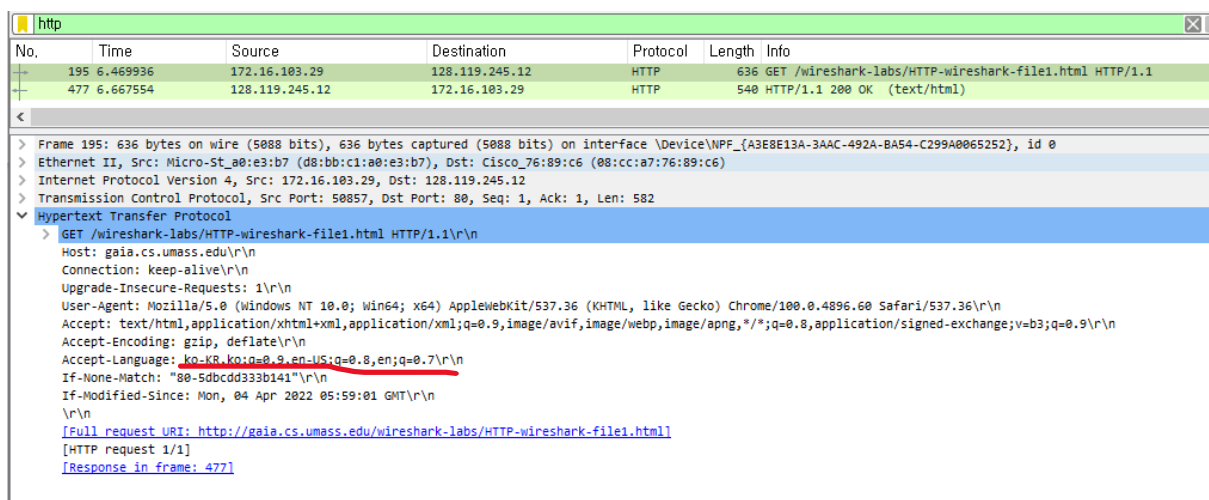
브라우저 상에서 확인 메시지를 확인했다.

1. HTTP의 버전은 아래 부분에서 Info 부분에 표시된 HTTP 버전이 모두 HTTP/1.1임을 통해 내 browser의 running되는 HTTP는 HTTP 1.1임을 알 수 있으며 또한 서버에서 running되는 HTTP버전 또한 HTTP version 1.1임을 알 수 있었다.



No.	Time	Source	Destination	Protocol	Length	Info
195	6.469936	172.16.103.29	128.119.245.12	HTTP	636	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
477	6.667554	128.119.245.12	172.16.103.29	HTTP	540	HTTP/1.1 200 OK (text/html)

2. 현재 서버에 받아들여지고 있는 언어는 아래 그림의 Accept-Language파트를 통해 확인할 수 있다. 현재 ko-KR(Korean-Republic of Korea), ko(Korean)와 en-US(US English), en(English)가 받아들여지고 있다는 것을 우리는 확인할 수 있다.



No.	Time	Source	Destination	Protocol	Length	Info
195	6.469936	172.16.103.29	128.119.245.12	HTTP	636	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
477	6.667554	128.119.245.12	172.16.103.29	HTTP	540	HTTP/1.1 200 OK (text/html)

> Frame 195: 636 bytes on wire (5088 bits), 636 bytes captured (5088 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50857, Dst Port: 80, Seq: 1, Ack: 1, Len: 582
> Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: ko-KR;q=0.9,en-US;q=0.8,en;q=0.7\r\nIf-None-Match: "80-5dbcdd33b141"\r\nIf-Modified-Since: Mon, 04 Apr 2022 05:59:01 GMT\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 477]

3. 아래를 보면 Source와 destination의 값이 각각 172.16.103.29와 128.119.245.12임을 알 수 있다.

이는 내 컴퓨터에서 gaia.cs.umass.edu 서버에 접속할 때 발생하였으므로 이를 바탕으로

나의 컴퓨터의 IP address는 172.16.103.29이며 gaia.cs.umass.edu server의 IP address는 128.119.245.12라는 것을 알 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
195	6.469936	172.16.103.29	128.119.245.12	HTTP	636	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

4. browser로 서버로부터 돌아온 status code값은 다음과 같다. 200 OK라는 내용을 통해 status code값으로 200이 돌아왔음을 확인할 수 있었다.

http

No.	Time	Source	Destination	Protocol	Length	Info
195	6.469936	172.16.103.29	128.119.245.12	HTTP	636	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
477	6.667554	128.119.245.12	172.16.103.29	HTTP	540	HTTP/1.1 200 OK (text/html)

<

> Frame 477: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0

> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29

> Transmission Control Protocol, Src Port: 80, Dst Port: 50857, Seq: 1, Ack: 583, Len: 486

> Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Tue, 05 Apr 2022 07:29:28 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Tue, 05 Apr 2022 05:59:02 GMT\r\n

Etag: "80-5d8e1f111581b"\r\n

Accept-Ranges: bytes\r\n

> Content-Length: 128\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: 0.197618000 seconds]

[Request in frame: 195]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

File Data: 128 bytes

> Line-based text data: text/html (4 lines)

No.	Time	Source	Destination	Protocol	Length	Info
1774	30.481093	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
1780	30.682870	128.119.245.12	172.16.103.29	HTTP	540	HTTP/1.1 200 OK (text/html)
1783	30.720938	172.16.103.29	128.119.245.12	HTTP	497	GET /favicon.ico HTTP/1.1
1785	30.922113	128.119.245.12	172.16.103.29	HTTP	538	HTTP/1.1 404 Not Found (text/html)

5. http.last_modified를 통해 아래를 확인하면 Last-modified가 Tue, 05 Apr 2022 07:29:28임을 알 수 있다. 이를 통해 2022년 4월 5일 화요일 7시 29분 28초에 발생했음을 확인할 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
477	6.667554	128.119.245.12	172.16.103.29	HTTP	540	HTTP/1.1 200 OK (text/html)

<p>> Frame 477: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0</p> <p>> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)</p> <p>> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29</p> <p>> Transmission Control Protocol, Src Port: 80, Dst Port: 50857, Seq: 1, Ack: 583, Len: 486</p> <p>> Hypertext Transfer Protocol</p> <p>> HTTP/1.1 200 OK\r\n</p> <p>Date: Tue, 05 Apr 2022 07:29:28 GMT\r\n</p> <p>Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n</p> <p>Last-Modified: Tue, 05 Apr 2022 05:59:02 GMT\r\n</p> <p>Etag: "80-5d8e1f111581b"\r\n</p> <p>Accept-Ranges: bytes\r\n</p> <p>> Content-Length: 128\r\n</p> <p>Keep-Alive: timeout=5, max=100\r\n</p> <p>Connection: Keep-Alive\r\n</p> <p>Content-Type: text/html; charset=UTF-8\r\n</p> <p>\r\n</p> <p>[HTTP response 1/1]</p> <p>[Time since request: 0.197618000 seconds]</p> <p>[Request in frame: 195]</p> <p>[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]</p> <p>File Data: 128 bytes</p> <p>> Line-based text data: text/html (4 lines)</p>													
--	--	--	--	--	--	--	--	--	--	--	--	--	--

6. 아래를 확인해 보면 Content-Length가 128라 기록됨을 알 수 있다. 이를 통해 128byte임을 알 수 있다.

```
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
195 6.469936 172.16.103.29 128.119.245.12 HTTP 636 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
477 6.667554 128.119.245.12 172.16.103.29 HTTP 540 HTTP/1.1 200 OK (text/html)

> Frame 477: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 50857, Seq: 1, Ack: 583, Len: 486
> Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 05 Apr 2022 07:29:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 05 Apr 2022 05:59:02 GMT\r\n
    ETag: "80-5d8e1f111581b"\r\n
    Accept-Ranges: bytes\r\n
    > Content-Length: 128\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: 0.197618000 seconds]
    [Request in frame: 195]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
  > Line-based text data: text/html (4 lines)
```

7. raw data는 packet listing된 window에 맞춰서 나오는 값이기 때문에 packet-listing된 window에 나오지 않는 header는 raw data를 검사하는 걸로는 볼 수 없다.

Wireshark · Packet 477 · 2-1.pcapng

```
> Frame 477: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}
> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 50857, Seq: 1, Ack: 583, Len: 486
> Hypertext Transfer Protocol
> Line-based text data: text/html (4 lines)
```

0000 d8 bb c1 a0 e3 b7 08 cc a7 76 89 c6 08 00 45 00V.....
0010 02 0e b0 ca 40 00 23 06 1c 6e 80 77 f5 0c ac 10 ...@.#..n-w....
0020 67 1d 00 50 c6 a9 fa 7b a2 5e 84 dc 46 81 50 18 g..P...{...F..P..
0030 00 ee 2b 38 00 00 48 54 54 50 2f 31 2e 31 20 32 ..+8..HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK..D ate: Tue
0050 2c 20 30 35 20 41 70 72 20 32 30 32 20 30 37 , 05 Apr 2022 07
0060 3a 32 39 3a 32 38 20 47 4d 54 0d 0a 53 65 72 76 :29:28 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
00a0 50 2f 37 2e 34 2e 32 38 20 6d 6f 64 5f 70 65 72 P/7.4.28 mod_per
00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi
00d0 66 69 65 64 3a 20 54 75 65 2c 20 30 35 20 41 70 fied: Tu e, 05 Ap
00e0 72 20 32 30 32 32 20 30 35 3a 35 39 3a 30 32 20 r 2022 0 5:59:02
00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 35 GMT..ETA g: "80-5
0100 64 62 65 31 66 31 31 31 35 38 31 62 22 0d 0a 41 dbe1f11 581b"..A
0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes..Con tent-Len
0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 ..Keep-A
0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5,
0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 ..Connec
0160 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0170 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 ..Conten t-Type:
0180 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; chars
0190 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8<htm
01a0 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f l>.Congr atulatio
01b0 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e ns. You 've down
01c0 6c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 loaded t he file
01d0 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e .http:// gaia.cs.
01e0 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 umass.ed u/wiresh
01f0 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 ark-lab s /HTTP-wi
0200 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 reshark. file1.ht
0210 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a</ht ml>..

닫기 도움말

다음은 <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>로 들어간 후 Wireshark를 통해 확인한 http에 관한 정보만을 display한 결과이다. 이를 바탕으로 Question 8~11의 질문을 분석한다.

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE field in your browser's HTTP GET request to the server.

실행 결과로서 이미 다운받았다는 것을 브라우저 내 텍스트를 통해 확인했다.

8. 브라우저에서 서버로 보내진 request에 대한 첫 HTTP GET에 대해서 IF-MODIFIED-SINCE는 확인할 수 없었다.

No.	Time	Source	Destination	Protocol	Length	Info
1034	8.510697	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1044	8.730918	128.119.245.12	172.16.103.29	HTTP	786	HTTP/1.1 200 OK (text/html)
1425	22.063454	172.16.103.29	128.119.245.12	HTTP	665	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1433	22.286444	128.119.245.12	172.16.103.29	HTTP	294	HTTP/1.1 304 Not Modified

> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49522, Dst Port: 80, Seq: 1, Ack: 1, Len: 497
> 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
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko-KR;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]
[Response in frame: 1044]

9. server에서 응답한 내용을 분석했을 때, 다음과 같은 Line-based text data를 직접적으로 (명시적으로) 확인할 수 있었다. 내부 내용은 html을 기반으로 작성된 file의 성공적인 다운로드를 알리는 메시지임을 확인했다.

No.	Time	Source	Destination	Protocol	Length	Info
1034	8.510697	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1044	8.730918	128.119.245.12	172.16.103.29	HTTP	786	HTTP/1.1 200 OK (text/html)
1425	22.063454	172.16.103.29	128.119.245.12	HTTP	665	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1433	22.286444	128.119.245.12	172.16.103.29	HTTP	294	HTTP/1.1 304 Not Modified


```

> Frame 1044: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 49522, Seq: 1, Ack: 498, Len: 732
> 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
  
```

10. 두번째 HTTP GET request에서는 IF-MODIFIED-SINCE가 관측되었다. 아래 캡처본에서 If-Modified-Since: Tue, 05 Apr 2022 05:19:02 GMT를 확인할 수 있다. 이를 통해 해당 header내 정보는 위와 같음을 알 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
1034	8.510697	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1044	8.730918	128.119.245.12	172.16.103.29	HTTP	786	HTTP/1.1 200 OK (text/html)
1425	22.063454	172.16.103.29	128.119.245.12	HTTP	665	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1433	22.286444	128.119.245.12	172.16.103.29	HTTP	294	HTTP/1.1 304 Not Modified


```

> Frame 1425: 665 bytes on wire (5320 bits), 665 bytes captured (5320 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 49521, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
> 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 Gecko) Chrome/100.0.4896.60 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  If-None-Match: W/"173-5d0e16206e912"\r\n
  If-Modified-Since: Tue, 05 Apr 2022 05:19:02 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/1]
  [Response in frame: 1433]
  
```


11. 캡처본에서 확인할 수 있듯이 2번째 HTTP GET에서 서버로부터 HTTP/1.1 304 Not Modified Response를 받을 수 있었다.(status code=304/phrase=Not modified Response) 이는 내용을 캐시에서 불러와 서버가 파일 내용을 반환할 필요 없었기 때문이다. 내부를 보면 Line-based text data가 해당 phase에선 확인할 수 없음을 알 수 있다. 즉, 이전에 받아온 것을 이용해 두번째에는 첫번째와 같은 완전한 packet이 아닌 일부 생략 및 변경 되어 보내짐을 알 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
1034	8.510697	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1044	8.730918	128.119.245.12	172.16.103.29	HTTP	786	HTTP/1.1 200 OK (text/html)
1425	22.063454	172.16.103.29	128.119.245.12	HTTP	665	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1433	22.286444	128.119.245.12	172.16.103.29	HTTP	294	HTTP/1.1 304 Not Modified


```

> Frame 1433: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29
> Transmission Control Protocol, Src Port: 80, Dst Port: 49521, Seq: 1, Ack: 612, Len: 240
< Hypertext Transfer Protocol
  < HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 03 Apr 2022 05:19:15 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.28 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: "173-5dbe16206e912"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.222990000 seconds]
    [Request in frame: 1425]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  
```

12~15번 문제를 풀기 전, 파일에 명시된 순서대로 다음과 같은 준비를 하였다.

Wireshark를 키고, brower에서 지정된 URL을 입력. 이후 Wireshark의 작동을 중지시키고 http를 입력해 다음과 같이 나타내어 주었다.

No.	Time	Source	Destination	Protocol	Length	Info
243	5.113435	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
251	5.312981	128.119.245.12	172.16.103.29	HTTP	535	HTTP/1.1 200 OK (text/html)

THE BILL OF RIGHTS Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

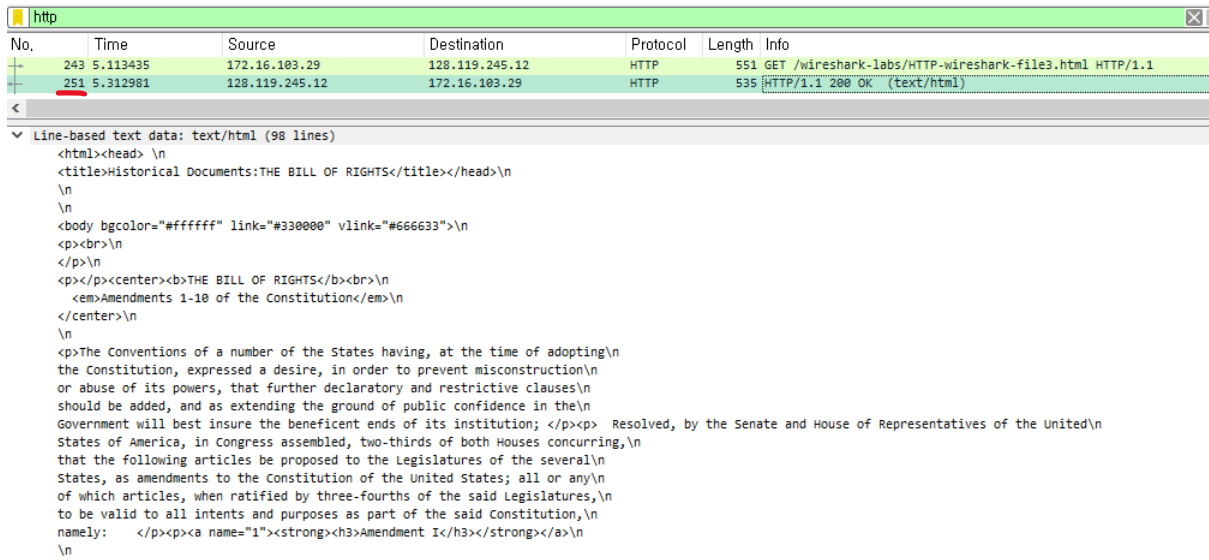
A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

위와 같이 브라우저 내에서 해당 텍스트를 확인하여 잘 진행되었음을 확인했다.

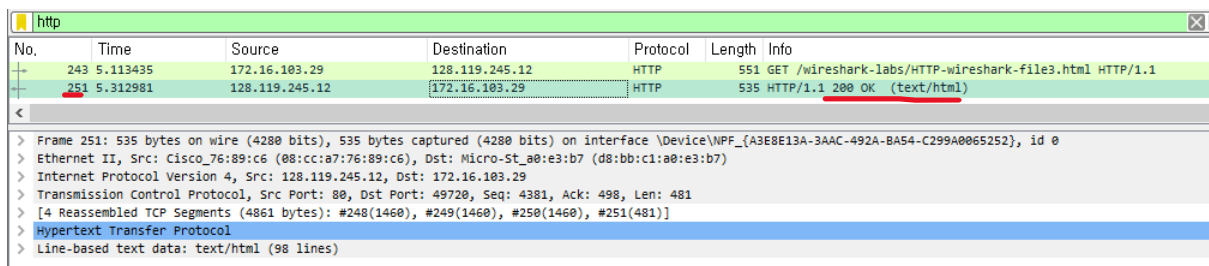
12. HTTP GET request는 브라우저로부터 한 번만 받게 된다. 또한 내부 내용에 Bill of rights에 대한 메시지가 포함되어 있다는 것을 접속했을 때 뜨는 텍스트와 Wireshark의 Line-based text data에서 확인할 수 있었다. 이를 확인할 수 있었던 No. 251인 packet에 이가 포함되어 있다는 것을 알 수 있다.



No.	Time	Source	Destination	Protocol	Length	Info
243	5.113435	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
251	5.312981	128.119.245.12	172.16.103.29	HTTP	535	HTTP/1.1 200 OK (text/html)

```
<html><head> \n<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n\n\n<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n<p><br>\n</p>\n<p></p><center><b>THE BILL OF RIGHTS</b><br>\n<em>Amendments 1-10 of the Constitution</em>\n</center>\n\n\n<p>The Conventions of a number of the States having, at the time of adopting\nthe Constitution, expressed a desire, in order to prevent misconstruction\nor abuse of its powers, that further declaratory and restrictive clauses\nshould be added, and as extending the ground of public confidence in the\nGovernment will best insure the beneficent ends of its institution; </p><p> Resolved, by the Senate and House of Representatives of the United\nStates of America, in Congress assembled, two-thirds of both Houses concurring,\nthat the following articles be proposed to the Legislatures of the several\nStates, as amendments to the Constitution of the United States; all or any\nof which articles, when ratified by three-fourths of the said Legislatures,\nbe valid to all intents and purposes as part of the said Constitution,\nnamely: </p><p><a name="1"><strong><h3>Amendment I</h3></strong></a>\n\n\n
```

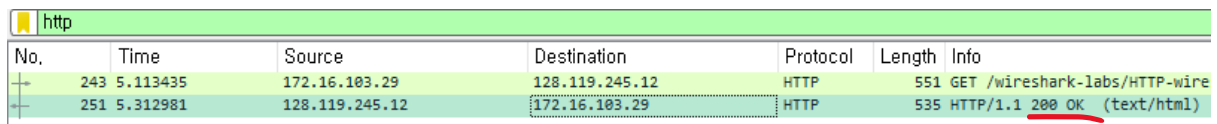
13. 아래 캡처본을 바탕으로 Info에서 확인할 수 있듯이 내 컴퓨터의 IP로 status code와 Phase로서 200 Ok를 전송해주는 No.251 packet이 HTTP GET request에 대해 응답하는 status code와 phrase를 포함하는 packet임을 알 수 있다.



No.	Time	Source	Destination	Protocol	Length	Info
243	5.113435	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
251	5.312981	128.119.245.12	172.16.103.29	HTTP	535	HTTP/1.1 200 OK (text/html)

```
> Frame 251: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0\n> Ethernet II, Src: Cisco_76:89:c6 (08:00:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)\n> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29\n> Transmission Control Protocol, Src Port: 80, Dst Port: 49720, Seq: 4381, Ack: 498, Len: 481\n> [4 Reassembled TCP Segments (4861 bytes): #248(1460), #249(1460), #250(1460), #251(481)]\n> Hypertext Transfer Protocol\n> Line-based text data: text/html (98 lines)
```

14. 아래 캡처본을 바탕으로 응답에 대한 status code와 phrase는 HTTP/1.1 200 OK을 통해 각각 200, OK임을 알 수 있다.



No.	Time	Source	Destination	Protocol	Length	Info
243	5.113435	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wire
251	5.312981	128.119.245.12	172.16.103.29	HTTP	535	HTTP/1.1 200 OK (text/html)

15. 아래 캡처본을 바탕으로 TCP가 얼마나 쓰였는지 알 수 있다. 3번에 나뉘어 TCP segment of reassembled PDU가 전달되었음을 알 수 있다. 즉, 3 개의 data-containing TCP segments가 single HTTP response와 text of the Bill of Rights에 필요했다는 것이다.

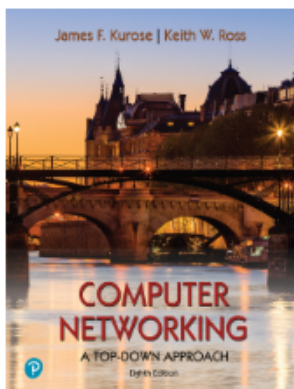
247	5.311744	128.119.245.12	172.16.103.29	TCP	60	80 → 49720 [ACK] Seq=1 Ack=498 Win=30336 Len=0	
248	5.312959	128.119.245.12	172.16.103.29	TCP	1514	80 → 49720 [ACK] Seq=1 Ack=498 Win=30336 Len=1460	TCP segment of a reassembled PDU
249	5.312981	128.119.245.12	172.16.103.29	TCP	1514	80 → 49720 [ACK] Seq=1461 Ack=498 Win=30336 Len=1460	TCP segment of a reassembled PDU
250	5.312981	128.119.245.12	172.16.103.29	TCP	1514	80 → 49720 [ACK] Seq=2921 Ack=498 Win=30336 Len=1460	TCP segment of a reassembled PDU
251	5.312981	128.119.245.12	172.16.103.29	HTTP	535	HTTP/1.1 200 OK (text/html)	
252	5.312997	172.16.103.29	128.119.245.12	TCP	54	49720 → 80 [ACK] Seq=498 Ack=4862 Win=262656 Len=0	

16-17을 풀기전 다음과 같은 준비를 해두었다.

Wireshark를 키고, browser에서 지정된 URL을 입력. 이후 Wireshark의 작동을 중지시키고 http를 입력해 다음과 같이 나타내어 주었다.



This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:



And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

위는 실행 결과로, 두개의 이미지와 URL을 비롯 적합한 결과가 나왔다.

2542	45.602700	172.16.103.29	128.119.245.12	HTTP	551	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	
2553	45.002954	128.119.245.12	172.16.103.29	HTTP	1355	HTTP/1.1 200 OK (text/html)	
2555	45.815925	172.16.103.29	128.119.245.12	HTTP	497	GET /pearson.png HTTP/1.1	
2563	46.013353	128.119.245.12	172.16.103.29	HTTP	745	HTTP/1.1 200 OK (PNG)	
2578	46.503152	172.16.103.29	178.79.137.164	HTTP	464	GET /8E_cover_small.jpg HTTP/1.1	
2595	46.788464	178.79.137.164	172.16.103.29	HTTP	225	HTTP/1.1 301 Moved Permanently	

Wireshark에 또한 다음과 같이 기록되었다.

16. Browser에서 보낸 Get메시지는 총 3개로 html파일과 png파일, jpg 파일을 받기 위해 메시지를 보냈다. html과 png 파일의 경우 128.119.245.12라는 주소에 요청되었다. Jpg 파일의 경우 178.79.137.164에 요청되었다.

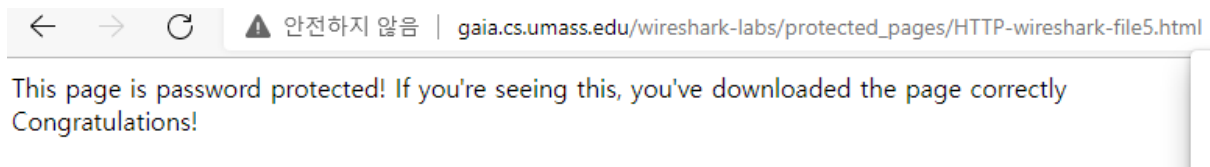
2542	45.602700	172.16.103.29	128.119.245.12	HTTP	551 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2553	45.802954	128.119.245.12	172.16.103.29	HTTP	1355 HTTP/1.1 200 OK (text/html)
2555	45.815925	172.16.103.29	128.119.245.12	HTTP	497 GET /pearson.png HTTP/1.1
2563	46.013353	128.119.245.12	172.16.103.29	HTTP	745 HTTP/1.1 200 OK (PNG)
2578	46.503152	172.16.103.29	178.79.137.164	HTTP	464 GET /8E_cover_small.jpg HTTP/1.1
2595	46.788464	178.79.137.164	172.16.103.29	HTTP	225 HTTP/1.1 301 Moved Permanently

17. 위의 결과를 바탕으로 동시에 처리된 것이 아닌, html, png, jpg순으로 요청하고 순서대로 (serially) 다운로드 되었다는 것을 알 수 있다. 즉, 두 개의 image는 parallel이 아니라 serially하게 브라우저에 다운로드 되었다.

2542	45.602700	172.16.103.29	128.119.245.12	HTTP	551 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
2553	45.802954	128.119.245.12	172.16.103.29	HTTP	1355 HTTP/1.1 200 OK (text/html)
2555	45.815925	172.16.103.29	128.119.245.12	HTTP	497 GET /pearson.png HTTP/1.1
2563	46.013353	128.119.245.12	172.16.103.29	HTTP	745 HTTP/1.1 200 OK (PNG)
2578	46.503152	172.16.103.29	178.79.137.164	HTTP	464 GET /8E_cover_small.jpg HTTP/1.1
2595	46.788464	178.79.137.164	172.16.103.29	HTTP	225 HTTP/1.1 301 Moved Permanently

18-19을 풀기전 다음과 같은 준비를 해두었다.

Wireshark를 키고, brower에서 지정된 URL을 입력. URL로 들어간 후, pop창에 username에는 wireshark-students를, password에는 network를 넣어주었다.



다음과 같은 완료 메시지를 확인하였다. 이후 Wireshark의 작동을 중지시키고 http를 입력해 다음과 같이 나타내어 주었다.

No.	Time	Source	Destination	Protocol	Length	Info
767	3.236964	172.16.103.29	128.119.245.12	HTTP	562	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
782	3.453563	128.119.245.12	172.16.103.29	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3529	24.598519	172.16.103.29	128.119.245.12	HTTP	647	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3813	24.807357	128.119.245.12	172.16.103.29	HTTP	544	HTTP/1.1 200 OK (text/html)

18. 브라우저로부터의 첫 HTTP GET메시지에 대한 응답으로 status code와 phrase가 HTTP/1.1 401 Unauthorized로 뜨는 것을 확인할 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
767	3.236964	172.16.103.29	128.119.245.12	HTTP	562	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
782	3.453563	128.119.245.12	172.16.103.29	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3529	24.598519	172.16.103.29	128.119.245.12	HTTP	647	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3813	24.807357	128.119.245.12	172.16.103.29	HTTP	544	HTTP/1.1 200 OK (text/html)

> Frame 782: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0

> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.103.29

> Transmission Control Protocol, Src Port: 80, Dst Port: 50651, Seq: 1, Ack: 509, Len: 717

> Hypertext Transfer Protocol

> Line-based text data: text/html (12 lines)

19. 첫 브라우저로부터의 HTTP GET메시지는 다음과 같았다.

No.	Time	Source	Destination	Protocol	Length	Info
767	3.236964	172.16.103.29	128.119.245.12	HTTP	562	GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html
782	3.453563	128.119.245.12	172.16.103.29	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3529	24.598519	172.16.103.29	128.119.245.12	HTTP	647	GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html
3813	24.807357	128.119.245.12	172.16.103.29	HTTP	544	HTTP/1.1 200 OK (text/html)

> Frame 767: 562 bytes on wire (4496 bits), 562 bytes captured (4496 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50651, Dst Port: 80, Seq: 1, Ack: 1, Len: 508
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html HTTP/1.1\r\n
 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/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 Safari/537.36 Edg/100.0.1185.29\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-files.html]
 [HTTP request 1/1]
 [Response in frame: 782]


그러나 브라우저로부터의 두번째 HTTP GET메시지에는 Authorization이라는 새로운 field가 전개되었음을 알 수 있다. 해당 field 내부에는 Credentials: wireshark-students:network라고 명시되어 있음도 확인할 수 있었다.

No.	Time	Source	Destination	Protocol	Length	Info
767	3.236964	172.16.103.29	128.119.245.12	HTTP	562	GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html
782	3.453563	128.119.245.12	172.16.103.29	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
3529	24.598519	172.16.103.29	128.119.245.12	HTTP	647	GET /wireshark-labs/protected_pages/HTTP-wireshark-files.html
3813	24.807357	128.119.245.12	172.16.103.29	HTTP	544	HTTP/1.1 200 OK (text/html)

> Frame 3529: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50667, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
▼ Hypertext Transfer Protocol
 > GET /wireshark-labs/protected_pages/HTTP-wireshark-files.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
 ▼ Authorization: Basic d2lyZXNoYXJrLXN0edwRlbnRzOm5ldHdvcm0=\r\n
 Credentials: wireshark-students:network
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.60 Safari/537.36 Edg/100.0.1185.29\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: ko,en;q=0.9,en-US;q=0.8\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-files.html]
 [HTTP request 1/1]
 [Response in frame: 3813]

Question #3(Wireshark_DNS_v7.0.pdf의 23개 문제 풀이-다음 결과들은 사전 조건에 맞추었다.)

1. nslookup을 이용해 Asia에 웹서버를 두는 Ip address를 얻어보고자 한다. 해당 정답에서
는 광운대학교 사이트를 이용하였다.

 선택 명령 프롬프트

```
Microsoft Windows [Version 10.0.19044.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Users\KimSangWoo>nslookup www.kw.ac.kr
서버:      kns.kornet.net
Address:  168.126.63.1

권한 없는 응답:
이름:      klas.kw.ac.kr
Address:   223.194.1.180
Aliases:   www.kw.ac.kr

C:\Users\KimSangWoo>
```

위와 같이 nslookup www.kw.ac.kr을 이용, 사이트의 ip address를 얻어낼 수 있었다. 광운
대학교의 IP address는 233.194.1.180이다.

아래는 wireshark를 통해 얻어낸 결과이다.

No.	Time	Source	Destination	Protocol	Length	Info
48	2.888707	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
49	2.812072	168.126.63.1	172.16.103.29	DNS	489	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa PTR kns.
50	2.812437	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x0002 A www.kw.ac.kr
51	2.816190	168.126.63.1	172.16.103.29	DNS	415	Standard query response 0x0002 A www.kw.ac.kr CNAME klas.kw.ac.kr A 2
52	2.817759	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x0003 AAAA www.kw.ac.kr
53	2.820649	168.126.63.1	172.16.103.29	DNS	142	Standard query response 0x0003 AAAA www.kw.ac.kr CNAME klas.kw.ac.kr
73	4.139332	172.16.103.29	168.126.63.1	DNS	78	Standard query 0xabd3 A edge.microsoft.com
74	4.142509	168.126.63.1	172.16.103.29	DNS	228	Standard query response 0xabd3 A edge.microsoft.com CNAME edge-micros

2. 유럽에 있는 대학의 authoritative DNS sever를 확인하기 위해 다음과 같은 명령어를 치고
결과를 확인했다. 이때 대학은 Cambridge 대학으로 정했다.

```
C:\Users\KimSangWoo>nslookup -type=NS www.cam.ac.uk
서버:      kns.kornet.net
Address:  168.126.63.1

cam.ac.uk
primary name server = primary.dns.cam.ac.uk
responsible mail addr = hostmaster.cam.ac.uk
serial = 1649156830
refresh = 1800 (30 mins)
retry = 900 (15 mins)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

다음과 같이 결과를 확인할 수 있었다. 이를 통해 Cambridge 대학의 authoritative DNS
server는 primary.dns.cam.ac.uk임을 알 수 있다.

3. 이를 바탕으로 얻은 DNS 서버 중 하나(primary.dns.cam.ac.uk을 이용)가 Yahoo mail에 대해 메일 서버에 Query되도록 nslookup 해주었다.

```
C:\Users\KimSangWoo>nslookup primary.dns.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
서버:      Unknown
Address:    119.161.15.251

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.

C:\Users\KimSangWoo>
```

해당 결과를 통해 IP address가 119.161.15.251임을 알 수 있었다.

4. <http://www.ietf.org>에 대한 wireshark의 캡처이다. 아래를 보면 각각 DNS query와 response message일 때 모두 UDP(User Datagram Protocol)로 보내짐을 확인할 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
105	4.998577	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x2ab5 A www.ietf.org
106	4.997355	168.126.63.1	172.16.103.29	DNS	459	Standard query response 0x2ab5 A www.ietf.org CNAME www.ietf.org
107	4.997763	172.16.103.29	104.16.45.99	TCP	66	52052 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
108	4.997940	172.16.103.29	104.16.45.99	TCP	66	52053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
109	5.001487	104.16.45.99	172.16.103.29	TCP	66	80 → 52052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
110	5.001523	104.16.45.99	172.16.103.29	TCP	66	80 → 52053 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
111	5.001530	172.16.103.29	104.16.45.99	TCP	54	52052 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
112	5.001550	172.16.103.29	104.16.45.99	TCP	54	52053 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
113	5.001638	172.16.103.29	104.16.45.99	HTTP	506	GET / HTTP/1.1

< Frame 105: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
 > Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
 > Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
 > User Datagram Protocol, Src Port: 51901, Dst Port: 53
 Source Port: 51901
 Destination Port: 53
 Length: 38
 Checksum: 0xfae4 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 11]
 > [Timestamps]
 UDP payload (30 bytes)

No.	Time	Source	Destination	Protocol	Length	Info
105	4.998577	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x2ab5 A www.ietf.org
106	4.997355	168.126.63.1	172.16.103.29	DNS	459	Standard query response 0x2ab5 A www.ietf.org CNAME www.ietf.org
107	4.997763	172.16.103.29	104.16.45.99	TCP	66	52052 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
108	4.997940	172.16.103.29	104.16.45.99	TCP	66	52053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
109	5.001487	104.16.45.99	172.16.103.29	TCP	66	80 → 52052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
110	5.001523	104.16.45.99	172.16.103.29	TCP	66	80 → 52053 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1
111	5.001530	172.16.103.29	104.16.45.99	TCP	54	52052 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
112	5.001550	172.16.103.29	104.16.45.99	TCP	54	52053 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
113	5.001638	172.16.103.29	104.16.45.99	HTTP	506	GET / HTTP/1.1

< Frame 106: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
 > Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
 > Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.16.103.29
 > User Datagram Protocol, Src Port: 53, Dst Port: 51901
 Source Port: 53
 Destination Port: 51901
 Length: 425
 Checksum: 0x43c2 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 11]
 > [Timestamps]
 UDP payload (417 bytes)

5. DNS response message의 Source Port와 DNS query message의 Destination Port를 확인해보았다. 각각 53, 53이 나오는 것을 확인할 수 있었다.

Wireshark packet capture analysis showing a DNS query and response. The filter is 'ip.addr == 172.16.103.29'.

No.	Time	Source	Destination	Protocol	Length	Info
105	4.990577	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x2ab5 A www.ietf.org
106	4.997355	168.126.63.1	172.16.103.29	DNS	459	Standard query response 0x2ab5 A www.ietf.org CNAME www.ietf.org
107	4.997763	172.16.103.29	104.16.45.99	TCP	66	52052 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
108	4.997940	172.16.103.29	104.16.45.99	TCP	66	52053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
109	5.001487	104.16.45.99	172.16.103.29	TCP	66	80 → 52052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1

Frame 105: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
 Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
 Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
 User Datagram Protocol, Src Port: 51901, Dst Port: 53
 Source Port: 51901
 Destination Port: 53
 Length: 38
 Checksum: 0xfae4 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 11]
 [Timestamps]
 UDP payload (30 bytes)

Frame 106: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
 Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
 Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.16.103.29
 User Datagram Protocol, Src Port: 53, Dst Port: 51901
 Source Port: 53
 Destination Port: 51901
 Length: 425
 Checksum: 0x43c2 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 11]
 [Timestamps]
 UDP payload (417 bytes)

6. Ipconfig /all을 통해 다음과 같이 DNS 서버의 IP(168.126.63.1)를 확인했다. 이는 WireShark의 Internet Protocol Version 4, Src:172.16.103.29, Dst: 168.126.63.1에서 확인할 수 있는 Dst: 168.126.63.1를 통해 문제에서 제시하는 DNS query message가 받아지는 IP address와 local DNS server의 IP address는 같은 IP address임을 알 수 있다.

```

DHCPv6 Iaid : 98089921
DHCPv6 클라이언트 DUID : 00-01-00-01-29-82-ED-73-D8-BB-C1-A0-E3-B7
DNS 서버 : 168.126.63.1
  
```

Wireshark packet capture analysis showing a DNS query. The filter is 'ip.addr == 172.16.103.29'.

No.	Time	Source	Destination	Protocol	Length	Info
105	4.990577	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x2ab5 A www.ietf.org
106	4.997355	168.126.63.1	172.16.103.29	DNS	459	Standard query response 0x2ab5 A www.ietf.org CNAME www.ietf.org
107	4.997763	172.16.103.29	104.16.45.99	TCP	66	52052 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
108	4.997940	172.16.103.29	104.16.45.99	TCP	66	52053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
109	5.001487	104.16.45.99	172.16.103.29	TCP	66	80 → 52052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1

Frame 105: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
 Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
 Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1

7. DNS query message를 확인해보면 DNS query의 Type이 type A임을 아래와 같이 확인할 수 있다. 또한 answers를 포함하지 않음 또한 확인이 가능했다.(Answer RRs가 0이다.)

```
Domain Name System (query)
Transaction ID: 0x2ab5
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: 106]
```

ip.addr == 172.16.103.29						
No.	Time	Source	Destination	Protocol	Length	Info
105	4.990577	172.16.103.29	168.126.63.1	DNS	72	Standard query 0x2ab5 A www.ietf.org
106	4.997355	168.126.63.1	172.16.103.29	DNS	459	Standard query response 0x2ab5 A www.ietf.org CNAME www.ietf
107	4.997763	172.16.103.29	104.16.45.99	TCP	66	52052 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
108	4.997940	172.16.103.29	104.16.45.99	TCP	66	52053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK
109	5.001487	104.16.45.99	172.16.103.29	TCP	66	80 → 52052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 S

```
> Frame 105: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_ao:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:00:07:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 51901, Dst Port: 53
  Source Port: 51901
  Destination Port: 53
  Length: 38
  Checksum: 0xfae4 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 11]
  [Timestamps]
  UDP payload (30 bytes)
Domain Name System (query)
Transaction ID: 0x2ab5
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 106]
```

8. DNS response message의 경우 아래와 같이 Answer RRs가 3만큼 존재함을 알 수 있었다. 즉, DNS response message는 3개의 answer를 가지고 있다는 것이다.

```
Domain Name System (response)
Transaction ID: 0x2ab5
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 3
Authority RRs: 5
Additional RRs: 10
Queries
Answers
> www.ietf.org: type CNAME, class IN, cname www.ietf.org.cdn.cloudflare.net
  Name: www.ietf.org
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 11 (11 seconds)
  Data length: 33
  CNAME: www.ietf.org.cdn.cloudflare.net
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
  Name: www.ietf.org.cdn.cloudflare.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 300 (5 minutes)
  Data length: 4
  Address: 104.16.45.99
> www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.44.99
  Name: www.ietf.org.cdn.cloudflare.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 300 (5 minutes)
  Data length: 4
  Address: 104.16.44.99
```

www.ietf.org의 이름(주소), 타입, class, Time to live, data length, CNAME을, www.ietf.org.cdn.cloudflare.net으로 된 나머지 두 answer는 이름(주소), 타입, class, Time to live, data length, IP address가 적혀 있음을 확인할 수 있다.

9. 다음을 보면 알 수 있듯이 SYN 패킷의 IP주소는 104.16.45.99로 이는 DNS response message에서 answer를 통해 확인할 수 있는 www.ietf.org.cdn.cloudflare.net의 ip_address와 동일하다. 이를 통해 SYN packet의 목적지 IP주소는 DNS response message에 제공된 IP주소와 일치함을 확인할 수 있다.

106	4.997355	168.126.63.1	172.16.103.29	DNS	459	Standard query response 0x2ab5 A www.ietf.org CNAME www.ietf.org
107	4.997763	172.16.103.29	104.16.45.99	TCP	66	52052 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
108	4.997940	172.16.103.29	104.16.45.99	TCP	66	52053 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
109	5.001487	104.16.45.99	172.16.103.29	TCP	66	80 → 52052 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_
110	5.001523	104.16.45.99	172.16.103.29	TCP	66	80 → 52053 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_
111	5.001530	172.16.103.29	104.16.45.99	TCP	54	52052 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
112	5.001550	172.16.103.29	104.16.45.99	TCP	54	52053 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
113	5.001638	172.16.103.29	104.16.45.99	HTTP	506	GET / HTTP/1.1

```

CNAME: www.ietf.org.cdn.cloudflare.net
www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.16.45.99
Name: www.ietf.org.cdn.cloudflare.net
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 300 (5 minutes)
Data length: 4
Address: 104.16.45.99

```

10. 이미지들은 www.ietf.org로부터 받아왔고 host는 cache된 주소를 통해 사용하기 때문에 추가적인 DNS queries는 발생하지 않는다.

No.	Time	Source	Destination	Protocol	Length	Info
80	4.535387	172.16.103.29	104.16.44.99	HTTP	501	GET / HTTP/1.1
84	4.553752	104.16.44.99	172.16.103.29	HTTP	357	HTTP/1.1 301 Moved Permanently

```

> Frame 80: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 104.16.44.99
> Transmission Control Protocol, Src Port: 52237, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
> Hypertext Transfer Protocol

```

(대표적으로 http만을 filter를 이용해 확인해도 image관련된 query는 발생하지 않았다.)

11. 다음은 아래 캡처본들을 통해 Destination port for DNS query message는 53임을, DNS response message의 Source port또한 53임을 알 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
26	1.424011	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
27	1.427792	168.126.63.1	172.16.103.29	DNS	423	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa
28	1.428547	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0002 A www.mit.edu
29	1.629708	168.126.63.1	172.16.103.29	DNS	484	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu

```

> Frame 28: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56874, Dst Port: 53
> Domain Name System (query)

```

No.	Time	Source	Destination	Protocol	Length	Info
26	1.424011	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
27	1.427792	168.126.63.1	172.16.103.29	DNS	423	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa PTR kns.kornet.net NS
28	1.428547	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0002 A www.mit.edu
29	1.629708	168.126.63.1	172.16.103.29	DNS	484	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME www.mit.edu
30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME www.mit.edu

```

> Frame 29: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.16.103.29
> User Datagram Protocol, Src Port: 53, Dst Port: 56874
> Domain Name System (response)

```

12. 아래와 같이 DNS query message를 받은 IP address는 168.126.63.1로 이는 ipconfig Wall로 얻을 수 있는 DNS서버의 값, 즉 내 컴퓨터의 default local DNS server의 IP address와 같다.

28	1.428547	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0002 A www.mit.edu
29	1.629708	168.126.63.1	172.16.103.29	DNS	484	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME
30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME

```
<
> Frame 28: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56874, Dst Port: 53
> Domain Name System (query)
```

```
DHCPv6 IAID : 98089921
DHCPv6 클라이언트 DUID : 00-01-00-01-29-82-ED-73-D8-BB-C1-A0-E3-B7
DNS 서버 : 168.126.63.1
```

13. 아래 캡처본에서 확인이 가능하듯, DNS query message의 Type은 A이다. 또한 “answers”는 포함하지 않음을 확인했다.(Answer RRs=0)

또한 이후 DNS query message의 Type은 AAAA이다. 이 또한 answers는 포함하지 않은 것을 Answer RRs=0으로 확인하였다.

28	1.428547	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0002 A www.mit.edu
29	1.629708	168.126.63.1	172.16.103.29	DNS	484	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME
30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME

```
<
> Frame 28: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56874, Dst Port: 53
> 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
      [Response In: 29]
```

30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME

```
<
> Frame 30: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56875, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0003
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > www.mit.edu: type AAAA, class IN
      [Response In: 33]
```

14. 캡처본과 같이 DNS response message는 2개로 A타입에 대한 Answer RRs값으로 3를 갖는다. 즉, answers는 총 3개이다. answers는 다음과 같은 값들을 가진다.

www.mit.edu: Name, Type, Class, Time to live, Data length, CNAME을 갖는다.

www.mit.edu.edgekey.net: Name, Type, Class, Time to live, Data length, CNAME을 갖는다.

e9566.dscb.akamaiedge.net: Name, Type, Class, Time to live, Data length, address를 가진다. 각각의 값들은 아래 캡처본을 따른다.

```
28 1.428547 172.16.103.29 168.126.63.1 DNS 71 Standard query 0x0002 A www.mit.edu
29 1.629708 168.126.63.1 172.16.103.29 DNS 484 Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.ak
30 1.631400 172.16.103.29 168.126.63.1 DNS 71 Standard query 0x0003 AAAA www.mit.edu
33 2.046203 168.126.63.1 172.16.103.29 DNS 524 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb

> Frame 29: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{A3E8E13A-3A4C-492A-B454-C299A0065252}, id 0
> Ethernet II, Src: Cisco_76:89:c6 (08:00:a7:76:89:c6), Dst: Micro-ST_08:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.16.103.29
> User Datagram Protocol, Src Port: 53, Dst Port: 56874
> Domain Name System (response)
  Transaction ID: 0x0002
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 8
  Additional RRs: 9
  > Queries
  > www.mit.edu: type A, class IN
  > 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: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 7 (7 seconds)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type A, class IN, addr 104.84.212.218
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 4
      Address: 104.84.212.218
  > Authoritative nameservers
```

캡처본과 같이 AAAA타입에 대한 DNS response message는 Answer RRs값으로 4를 갖는다. 즉, answers는 총 4개이다. answers는 다음과 같은 값들을 가진다.

www.mit.edu: Name, Type, Class, Time to live, Data length, CNAME을 갖는다.

www.mit.edu.edgekey.net: Name, Type, Class, Time to live, Data length, CNAME을 갖는다.

e9566.dscb.akamaiedge.net(2개): Name, Type, Class, Time to live, Data length, address를 가진다. 각각의 값들은 아래 캡처본을 따른다.

```
33 2.046203 168.126.63.1 172.16.103.29 DNS 524 Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb

> User Datagram Protocol, Src Port: 53, Dst Port: 56875
> Domain Name System (response)
  Transaction ID: 0x0003
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 4
  Authority RRs: 8
  Additional RRs: 9
  > Queries
  > www.mit.edu: type AAAA, class IN
  > 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: 1800 (30 minutes)
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
    > www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 7 (7 seconds)
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:9800:3b9::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 16
      AAAA Address: 2600:1417:9800:3b9::255e
    > e9566.dscb.akamaiedge.net: type AAAA, class IN, addr 2600:1417:9800:39a::255e
      Name: e9566.dscb.akamaiedge.net
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 20 (20 seconds)
      Data length: 16
      AAAA Address: 2600:1417:9800:39a::255e
```

15. Screenshot은 다음과 같다.

dns						
No.	Time	Source	Destination	Protocol	Length	Info
26	1.424011	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
27	1.427792	168.126.63.1	172.16.103.29	DNS	423	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa PTR kns
28	1.428547	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0002 A www.mit.edu
29	1.629708	168.126.63.1	172.16.103.29	DNS	484	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu.edgekey
30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.edu.ec

<

> Frame 28: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0

> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)

> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1

> User Datagram Protocol, Src Port: 56874, Dst Port: 53

✓ 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

[\[Response In: 29\]](#)

dns						
No.	Time	Source	Destination	Protocol	Length	Info
26	1.424011	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
27	1.427792	168.126.63.1	172.16.103.29	DNS	423	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa F
28	1.428547	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0002 A www.mit.edu
29	1.629708	168.126.63.1	172.16.103.29	DNS	484	Standard query response 0x0002 A www.mit.edu CNAME www.mit.edu
30	1.631400	172.16.103.29	168.126.63.1	DNS	71	Standard query 0x0003 AAAA www.mit.edu
33	2.046203	168.126.63.1	172.16.103.29	DNS	524	Standard query response 0x0003 AAAA www.mit.edu CNAME www.mit.

<

> Frame 29: 484 bytes on wire (3872 bits), 484 bytes captured (3872 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0

> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)

> Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.16.103.29

> User Datagram Protocol, Src Port: 53, Dst Port: 56874

✓ Domain Name System (response)

Transaction ID: 0x0002

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 8

Additional RRs: 9

✓ Queries

> www.mit.edu: type A, class IN

✓ 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: 1800 (30 minutes)

Data length: 25

CNAME: www.mit.edu.edgekey.net

✓ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net

Name: www.mit.edu.edgekey.net

Type: CNAME (Canonical NAME for an alias) (5)

Class: IN (0x0001)

Time to live: 7 (7 seconds)

Data length: 24

CNAME: e9566.dscb.akamaiedge.net

✓ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.84.212.218

Name: e9566.dscb.akamaiedge.net

Type: A (Host Address) (1)

Class: IN (0x0001)

Time to live: 20 (20 seconds)

Data length: 4

Address: 104.84.212.218

16. 다음 캡처본에서 DNS query message가 받아진 IP address는 168.126.63.1임을 알 수 있다. 이는 ipconfig /all을 통해 얻을 수 있는 내 컴퓨터의 default local DNS 서버의 IP address와 같음을 알 수 있었다.

42	3.583296	172.16.103.29	168.126.63.1	DNS	67 Standard query 0x0002 NS mit.edu
44	3.649064	168.126.63.1	172.16.103.29	DNS	330 Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS ns1-3
102	9.302019	172.16.103.29	168.126.63.1	DNS	77 Standard query 0xbc2e A beacons3.gvt2.com
104	9.310687	168.126.63.1	172.16.103.29	DNS	348 Standard query response 0xbc2e A beacons3.gvt2.com A 172.217.161.35

```
> Frame 42: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_00:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56679, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      [Response In: 44]
```

```
DHCPv6 IAID : 98089921
DHCPv6 클라이언트 DUID : 00-01-00-01-29-82-ED-73-D8-BB-C1-A0-E3-B7
DNS 서버 : 168.126.63.1
```

17. DNS query message는 Queries내 값을 통해 NS type을 갖는 걸 알 수 있다. Answer RRs가 0인 Answer가 없는 형태를 취한다.

42	3.583296	172.16.103.29	168.126.63.1	DNS	67 Standard query 0x0002 NS mit.edu
44	3.649064	168.126.63.1	172.16.103.29	DNS	330 Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS ns1-3
102	9.302019	172.16.103.29	168.126.63.1	DNS	77 Standard query 0xbc2e A beacons3.gvt2.com
104	9.310687	168.126.63.1	172.16.103.29	DNS	348 Standard query response 0xbc2e A beacons3.gvt2.com A 172.217.161.35

```
> Frame 42: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_00:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56679, Dst Port: 53
▼ Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ mit.edu: type NS, class IN
      Name: mit.edu
      [Name Length: 7]
      [Label Count: 2]
      Type: NS (authoritative Name Server) (2)
      Class: IN (0x0001)
      [Response In: 44]
```

18. 다음과 같이 response message를 제공하는 MIT nameservers는 아래 캡처에서 확인할 수 있듯이 Eur5.akam.net, use2.akam.net, use5.akam.net, usw2.akam.net, asia1.akam.net, asia2.akam.net, ns1-27.akam.net과 ns1-173.akam.net이다. 이때 이들은 addr, 즉 nameserver들의 IP address 제공해주고 있음을 확인할 수 있다.

No.	Time	Source	Destination	Protocol	Length	Info
40	3.575576	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
41	3.581302	168.126.63.1	172.16.103.29	DNS	489	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa PTR kns.
42	3.583296	172.16.103.29	168.126.63.1	DNS	67	Standard query 0x0002 NS mit.edu
44	3.649064	168.126.63.1	172.16.103.29	DNS	330	Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS ns1-37.
102	9.302019	172.16.103.29	168.126.63.1	DNS	77	Standard query 0xbc2e A beacons3.gvt2.com
104	9.310687	168.126.63.1	172.16.103.29	DNS	348	Standard query response 0xbc2e A beacons3.gvt2.com A 172.217.161.35

> Frame 44: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Cisco_76:89:c6 (08:cc:a7:76:89:c6), Dst: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7)
> Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.16.103.29
> User Datagram Protocol, Src Port: 53, Dst Port: 56679
▼ Domain Name System (response)
Transaction ID: 0x0002
> Flags: 0x8100 Standard query response, No error
Questions: 1
Answer RRs: 8
Authority RRs: 0
Additional RRs: 6
> Queries
▼ Answers
> mit.edu: type NS, class IN, ns eur5.akam.net
> mit.edu: type NS, class IN, ns ns1-37.akam.net
> mit.edu: type NS, class IN, ns asia2.akam.net
> mit.edu: type NS, class IN, ns asia1.akam.net
> mit.edu: type NS, class IN, ns usw2.akam.net
> mit.edu: type NS, class IN, ns ns1-173.akam.net
> mit.edu: type NS, class IN, ns use2.akam.net
> mit.edu: type NS, class IN, ns use5.akam.net
▼ Additional records
> eur5.akam.net: type A, class IN, addr 23.74.25.64
> use2.akam.net: type A, class IN, addr 96.7.49.64
> use5.akam.net: type A, class IN, addr 2.16.40.64
> usw2.akam.net: type A, class IN, addr 184.26.161.64
> asia1.akam.net: type A, class IN, addr 95.100.175.64
> asia2.akam.net: type A, class IN, addr 95.101.36.64

19. 스크린샷은 다음과 같다.

*이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
40	3.575576	172.16.103.29	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
41	3.581302	168.126.63.1	172.16.103.29	DNS	489	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa PT
42	3.583296	172.16.103.29	168.126.63.1	DNS	67	Standard query 0x0002 NS mit.edu
44	3.649064	168.126.63.1	172.16.103.29	DNS	330	Standard query response 0x0002 NS mit.edu NS eur5.akam.net NS n
102	9.302019	172.16.103.29	168.126.63.1	DNS	77	Standard query 0xbc2e A beacons3.gvt2.com
104	9.310687	168.126.63.1	172.16.103.29	DNS	348	Standard query response 0xbc2e A beacons3.gvt2.com A 172.217.16

> Frame 42: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}, id 0
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 56679, Dst Port: 53
▼ Domain Name System (query)
Transaction ID: 0x0002
> Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
> Queries
[Response In: 44]

20. DNS query message가 받아진 IP address는 다음 캡처본에서 확인할 수 있다. 캡처본에 따라 bitsy.mit.edu로의 DNS query message는 168.126.63.1로, www.aiit.or.kr로의 DNS query message는 18.0.72.3로 가고 있음을 확인했다. Bitsy.mit.edu의 경우 내 default local DNS server의 IP address와 같지만 www.aiit.or.kr의 경우 bitsy.mit.edu로부터 받아온 IP address이기 때문에 다르다.

No.	Time	Source	Destination	Protocol	Length	Info
72	3.197604	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
73	3.235808	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
74	3.263834	168.126.63.1	172.16.103.29	DNS	548	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
75	3.265099	172.16.103.29	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

DHCPv6 IAID . . . : 98089921
DHCPv6 클라이언트 DUID . . . : 00-01-00-01-29-82-ED-73-D8-BB-C1-A0-E3-B7
DNS 서버 . . . : 168.126.63.1

```

```

C:\Users\KimSangWoo>nslookup www.aiit.or.kr bitsy.mit.edu
DNS request timed out.
    timeout was 2 seconds.
서버:      Unknown
Address:   18.0.72.3

```

21. 캡처본의 내용을 통해 bitsy.mit.edu로의 DNS query의 Type은 A임을 확인할 수 있다. 또한 Answer RRs는 0이므로 Answer는 포함하지 않는다.

72	3.197604	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
73	3.235808	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
74	3.263834	168.126.63.1	172.16.103.29	DNS	548	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
75	3.265099	172.16.103.29	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr


```

> Frame 72: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 49789, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x277b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > bitsy.mit.edu: type A, class IN
    [Response in: 74]

```


73	3.235808	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
74	3.263834	168.126.63.1	172.16.103.29	DNS	548	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
75	3.265099	172.16.103.29	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr


```

> Frame 73: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 49789, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x277b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    > bitsy.mit.edu: type A, class IN
    [Retransmitted request. Original request in: 72]
    [Retransmission: True]

```


단, www.aiit.or.kr의 경우 A와 AAAA 타입의 형태로 2번씩 보내졌으며 이들 또한 Answer RRs가 0, 즉 answer는 포함하지 않는 모습이다.

109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

> Frame 109: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-B
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 49791, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0002
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.aiit.or.kr: type A, class IN

```

138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

> Frame 138: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-B
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 49792, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.aiit.or.kr: type AAAA, class IN

```

166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

```

> Frame 166: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-B
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 49793, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0004
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.aiit.or.kr: type A, class IN

```

187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr
-----	-----------	---------------	-----------	-----	----	---

```

> Frame 187: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-B
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 49794, Dst Port: 53
> Domain Name System (query)
  Transaction ID: 0x0005
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  > Queries
    > www.aiit.or.kr: type AAAA, class IN

```

또한 PTR타입의 Query message또한 보내졌다는 것을 확인했다. 이 또한 Answer RRs가 0인 Answer를 갖지 않는 message이다.(이는 무시하는 것이지만 추가적으로 언급하였다.)

75	3.265099	172.16.103.29	18.0.72.3	DNS	82	Standard query	0x0001	PTR	3.72.0.18.in-addr.arpa
76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response	0x277b	A	bitsy.mit.edu A 18.0.72.3 NS
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0002	A	www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0003	AAAA	www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0004	A	www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0005	AAAA	www.aiit.or.kr

```

> Frame 75: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A0065252}
> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:cl:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)
> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 18.0.72.3
> User Datagram Protocol, Src Port: 49790, Dst Port: 53
✓ Domain Name System (query)
  Transaction ID: 0x0001
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ✓ Queries
    > 3.72.0.18.in-addr.arpa: type PTR, class IN

```

22. DNS response message의 경우 둘 다 캡처본에서 확인 할 수 있듯이 1개의 Answer를 가진다는 것을 Answer RRs를 통해 확인 할 수 있었다. 이 Answer는 아래와 같이 Name, Type, Class, Time to live, Data length, Address를 포함하고 있다.

74	3.263834	168.126.63.1	172.16.103.29	DNS	548	Standard query response	0x277b	A	bitsy.mit.edu A 18.0.72.3 NS
75	3.265099	172.16.103.29	18.0.72.3	DNS	82	Standard query	0x0001	PTR	3.72.0.18.in-addr.arpa
76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response	0x277b	A	bitsy.mit.edu A 18.0.72.3 NS
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0002	A	www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0003	AAAA	www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0004	A	www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0005	AAAA	www.aiit.or.kr

```

Questions: 1
Answer RRs: 1
Authority RRs: 13
Additional RRs: 14
✓ Queries
  > bitsy.mit.edu: type A, class IN
✓ Answers
  ✓ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
    Name: bitsy.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 4
    Address: 18.0.72.3
  > Authoritative nameservers
  > Additional records
  [Request In: 72]
  [Time: 0.066230000 seconds]

```

76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response	0x277b	A	bitsy.mit.edu A 18.0.72.3
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0002	A	www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0003	AAAA	www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0004	A	www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query	0x0005	AAAA	www.aiit.or.kr

```

> Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 8
Additional RRs: 11
✓ Queries
  > bitsy.mit.edu: type A, class IN
✓ Answers
  ✓ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
    Name: bitsy.mit.edu
    Type: A (Host Address) (1)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 4
    Address: 18.0.72.3

```

단 www.aiit.or.kr에 대해서는 DNS response message를 받지 못하여 확인 할 수 없었다.

23. 스크린 샷은 다음과 같다.

No.	Time	Source	Destination	Protocol	Length	Info
72	3.197604	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
73	3.235808	172.16.103.29	168.126.63.1	DNS	73	Standard query 0x277b A bitsy.mit.edu
74	3.263834	168.126.63.1	172.16.103.29	DNS	548	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
75	3.265099	172.16.103.29	18.0.72.3	DNS	82	Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
76	3.310862	168.126.63.1	172.16.103.29	DNS	468	Standard query response 0x277b A bitsy.mit.edu A 18.0.72.3
109	5.272934	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0002 A www.aiit.or.kr
138	7.273521	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0003 AAAA www.aiit.or.kr
166	9.278286	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0004 A www.aiit.or.kr
187	11.284128	172.16.103.29	18.0.72.3	DNS	74	Standard query 0x0005 AAAA www.aiit.or.kr

> Frame 72: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface \Device\NPF_{A3E8E13A-3AAC-492A-BA54-C299A006525}

> Ethernet II, Src: Micro-St_a0:e3:b7 (d8:bb:c1:a0:e3:b7), Dst: Cisco_76:89:c6 (08:cc:a7:76:89:c6)

> Internet Protocol Version 4, Src: 172.16.103.29, Dst: 168.126.63.1

> User Datagram Protocol, Src Port: 49789, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x277b

> Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

> bitsy.mit.edu: type A, class IN

[\[Response In: 74\]](#)

결론 및 고찰

위 과제를 하면서 Wireshark의 사용법 및 Http와 DNS환경에서 네트워크가 어떤 식으로 동작하는지를 확인할 수 있었다. 특히 보안이 걸려있을 때, 이미지를 받아올 때 등 다양한 환경에서의 네트워크를 대상으로 관찰하였다는 점에서 이번 과제가 더욱 보람이 있었다고 생각한다. 이를 통해 네트워크가 돌아가는 구조에 대한 이해도를 높일 수 있었고, Status나 Phrase를 확인하며 에러를 찾거나 현 상태에 대한 대비를 하는 등, 앞으로의 개발에 영향을 크게 줄 수 있을 만한 정보들도 얻을 수 있었다.