컴퓨터네트워크

과제 제목: Wireshark Assignment

강의 시간: 화 5교시, 목 6교시
교수님 : 이 혁 준 교수님
소 속: 컴퓨터정보공학부
학 번: 2019202021
이 름: 정 성 엽
제 출 일: 2023/4/10

1. 서론(5줄 이상)

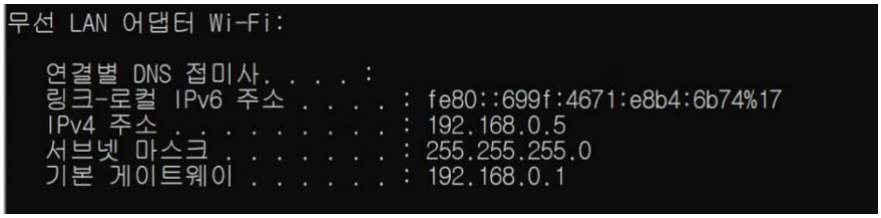
   패킷 캡처를 통해 패킷 분석을 할 수 있는 툴인 wireshark를 설치하고 이를 실행해 본다. 또한 필터 없이 패킷 리스트를 보았을 때 source 또는 destination이 자신의 ip와 일치하는 것이 있는지 확인해본다. 후에 간단한 예제를 통해 브라우저에서 특정 페이지를 들어갔을 때 html을 get 요청했을 때 response 결과가 어떻게 되는지 실습을 통해 확인하고 패킷리스트와 그 상세사항에 어떤 정보가 포함되어 제공되는지 확인한다. 또한 특정 명령어를 실행했을 때 해당 DNS의 query와 response message를 확인해보며, 각 question에 대한 answer를 확인한다.

2. 본문

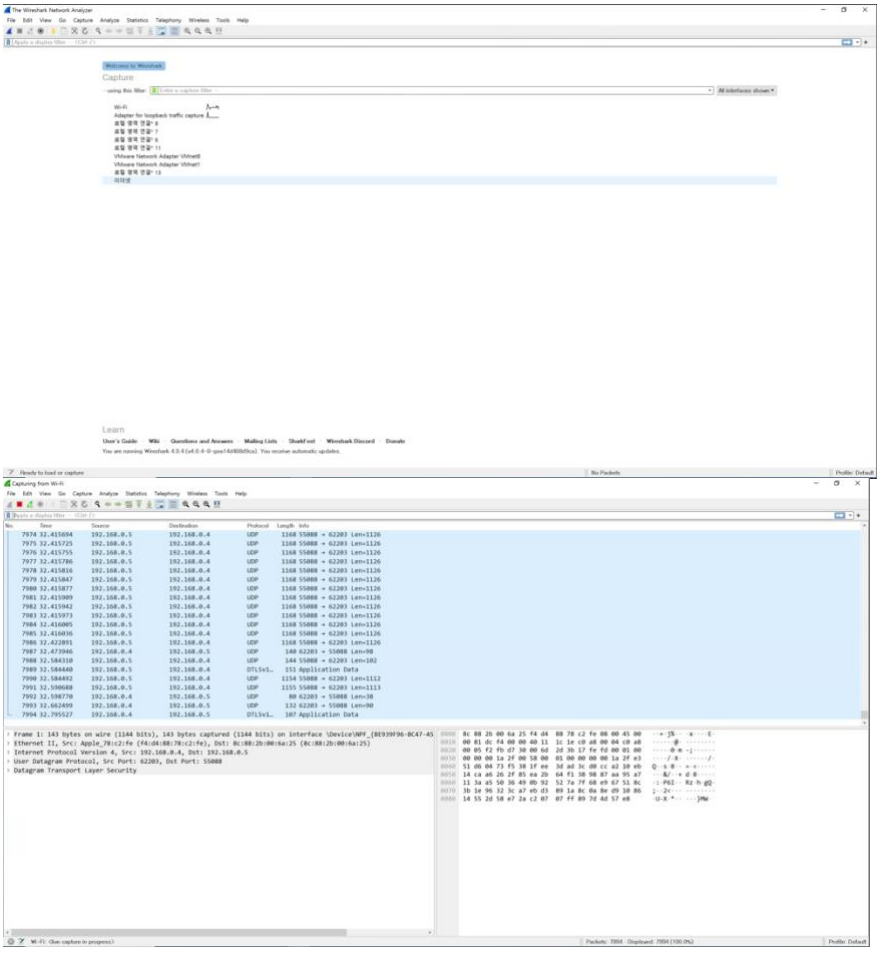
   A. Question #1

      i. Windows

         1) IP 화면



         2) Wireshark

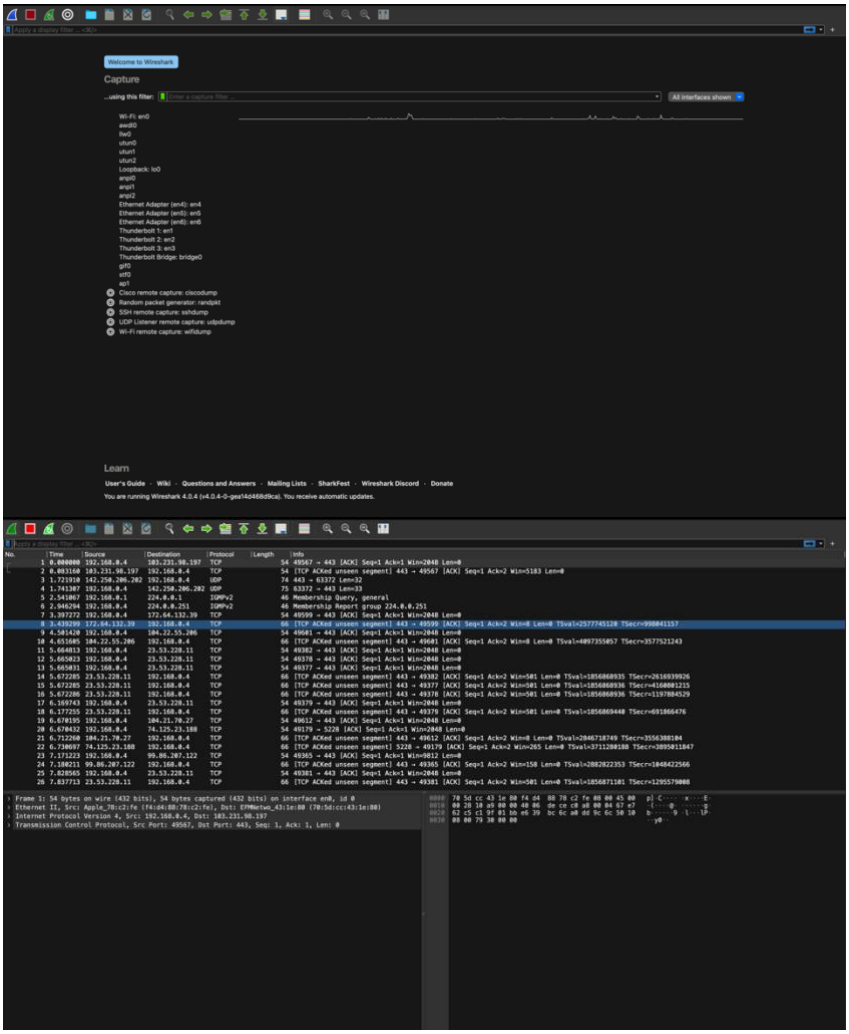


      ii. macOS

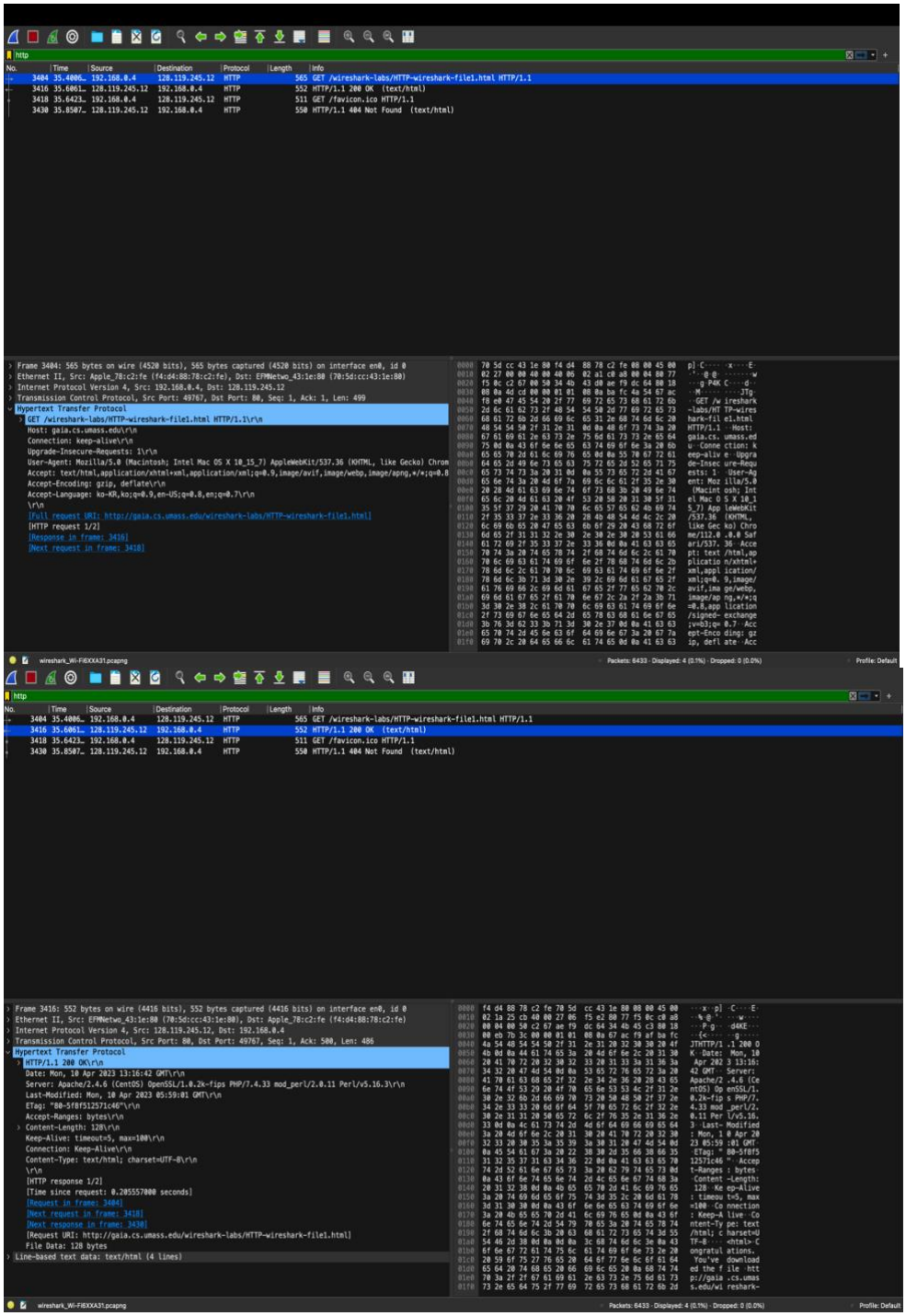
         1) IP 화면

```
Last login: Mon Apr 10 22:00:29 on ttys000
jsy@jeongseong-yeob-ui-MacBookPro ~ % ipconfig getifaddr en0
192.168.0.4
jsy@jeongseong-yeob-ui-MacBookPro ~ %
```

2) Wireshark

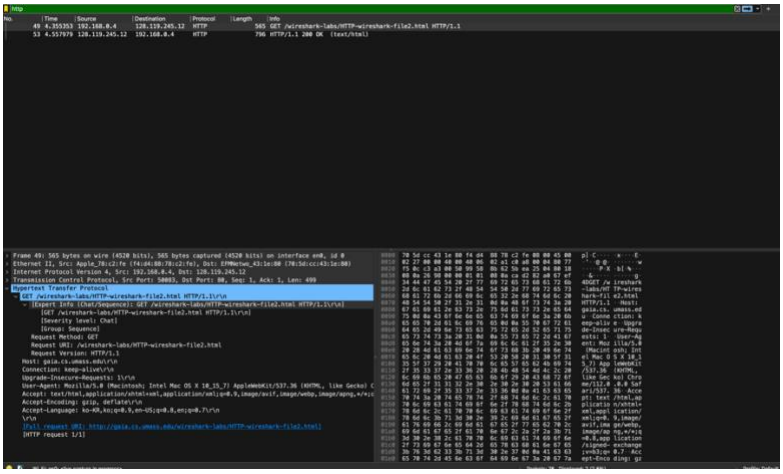


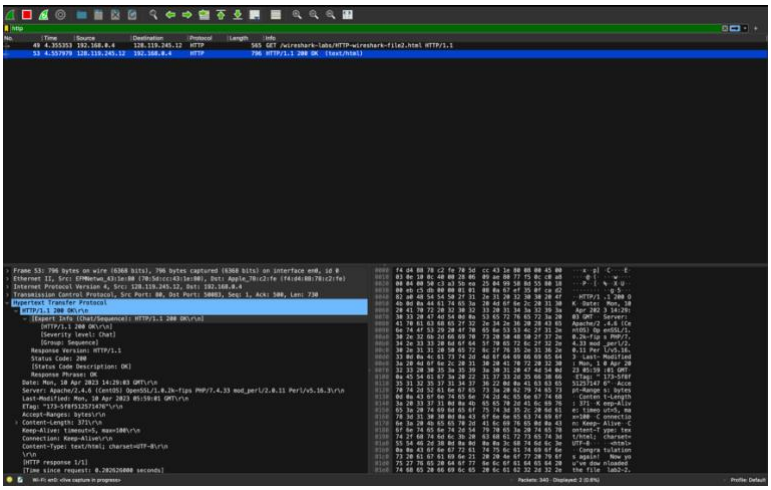
B. Question #2



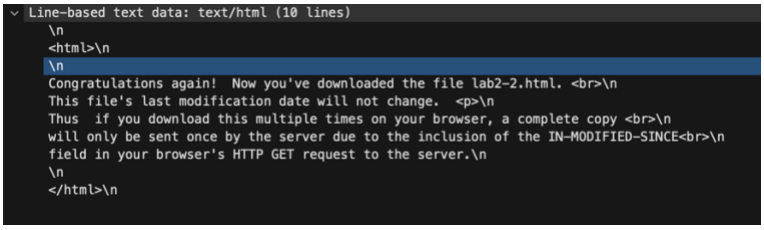
1. Is your browser running HTTP version 1.0 or 1.1? what version of HTTP is the server running
   - 브라우저와 서버 모두 1.1 버전을 사용하고 있다.
2. What languages (if any) does your browser indicate that it can accept to the server?
   - ko-KR 을 사용하고 있다.
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   - client(computer) : 192.168.0.4 // server : 128.119.245.12

4. What is the status code returned from the server to your browser?
   - 200 ok 가 반환되었다.
5. When was the HTML file that you are retrieving last modified at the server?
   - Last-Modified: Mon, 10 Apr 2023 05:59:01 GMT₩r₩n 이 있다.
6. How many bytes of content are being returned to your browser?
   - Content-Length: 128 bytes 브라우저로 반환되었다.
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
   - packet content window 에 표시되지 않는 헤더는 보이지 않는다.

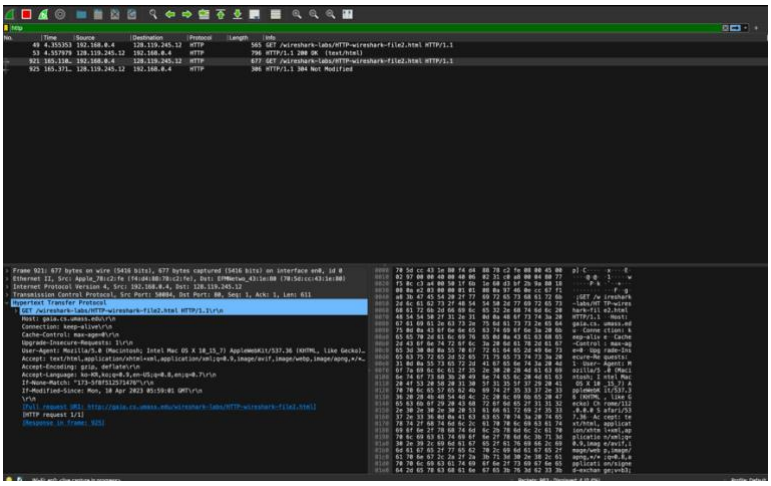




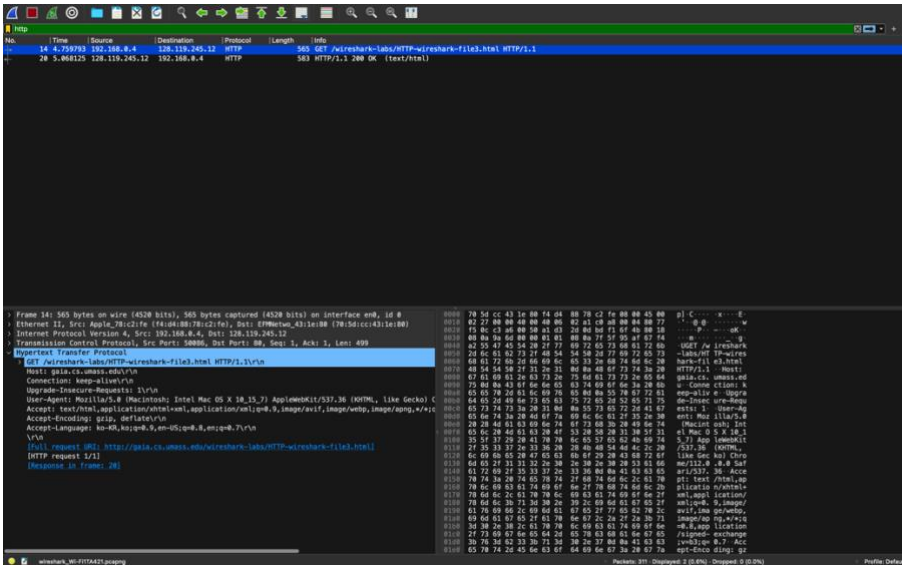
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
   - 처음 실행했을 때는 보이지 않는다.
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

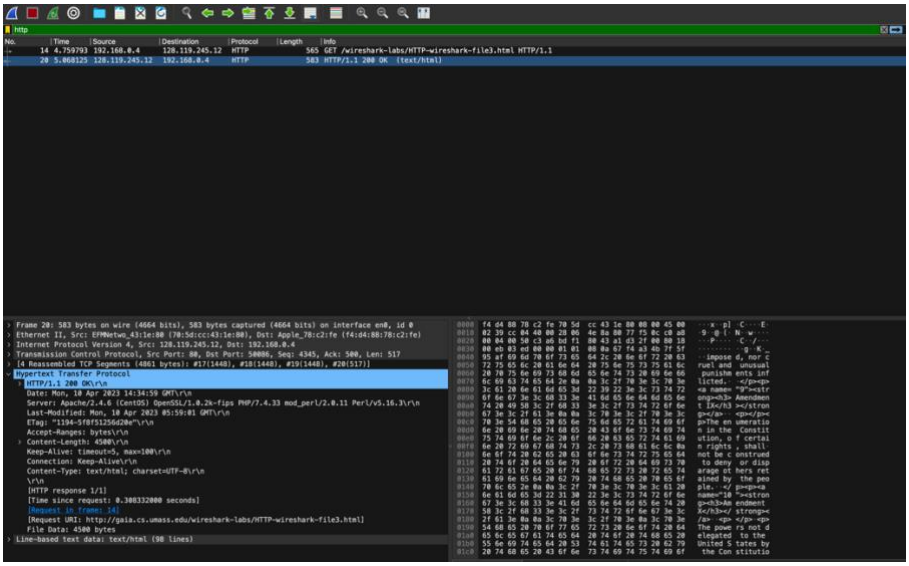


-
- Line-based text data: text/html (10 lines)에서 확인 가능하다.

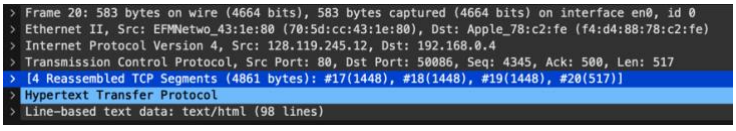


10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?
    - 두 번째 요청에서는 If-Modified-Since: Mon, 10 Apr 2023 05:59:01 GMT₩r₩n 이 생겼다.
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
    - http status 코드는 304: Not Modified 로 브라우저가 서버가 아닌 캐시에서 파일을 로드했기 때문에 서버가 파일 콘텐츠를 반환하지 않았다.

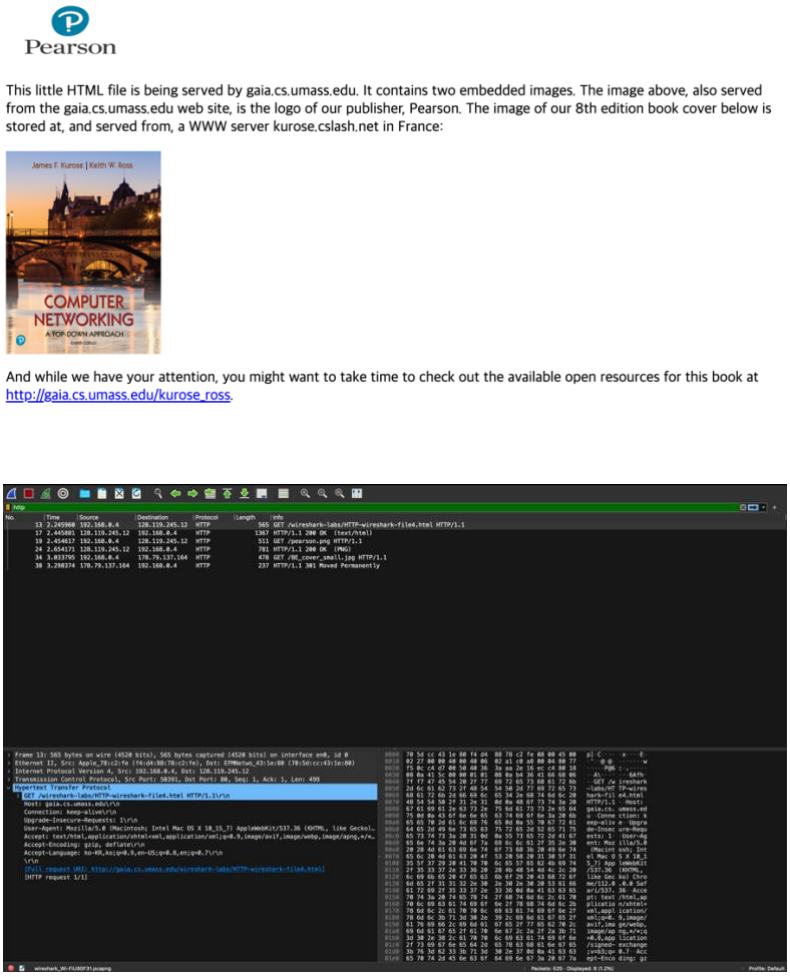




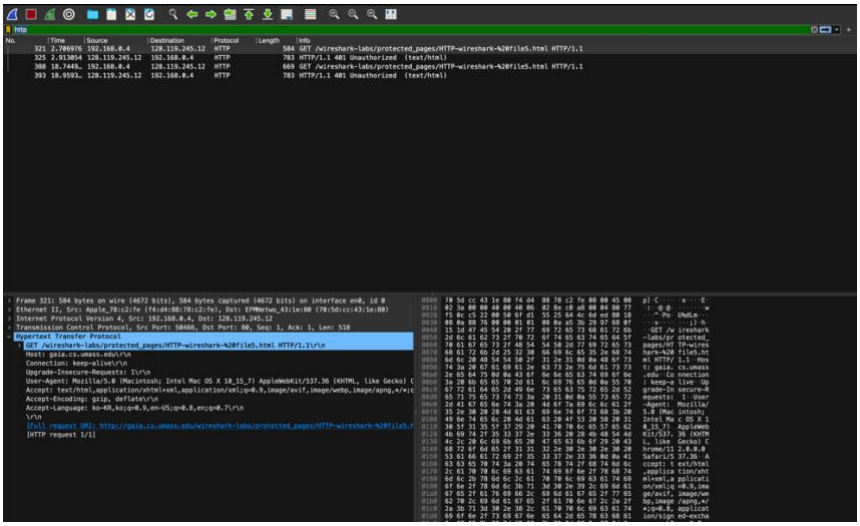
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
    - 한번만 보냈다. Packet number 는 14 이다.
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    - Packet number 20 이다.
14. What is the status code and phrase in the response?
    - status code 는 200 이고 phrase 는 ok 이다.
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
    -



- 4 개의 tcp segments 로 데이터는 브라우저로 보내졌고 그 다음 재조립되었다.



16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    - 브라우저는 HTTP GET request messages 를 3 번 보냈고 처음 페이지 주소는 128.119.245.12, pearson.png 사진은 128.192.245.12, 8E_cover_small.jpg 사진은 178.79.137.164 로 보냈다.
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.
    - 브라우저에서 이미지는 순차적으로 다운로드 되었다. Packet List 의 순서를 보면 첫 번째 이미지를 request 하고 첫 번째 이미지가 받았으며, 그 후 두 번째 이미지를 request 하고 두 번째 이미지를 받았기 때문이다. 만약 동시에 다운로드 된다면 request 가 연속적으로 나타나야 한다.



18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
    - status code 는 401 이고 phrase 는 Unauthorized 로 반응했다.
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    -
    ```
    Hypertext Transfer Protocol
      GET /wireshark-labs/protected_pages/HTTP-wireshark-%20file5.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 anVuZyBzdW5nIHllb2I6aGVsbG93b3JsZA==\r\n
        Credentials: jung sung yeob:helloworld
    ```
    - 브라우저가 HTTP GET 을 보냈을 때, 내용에는 Authorization 가 추가되어 user name 과 password 가 포함되어 있다.

C. Question #3

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?
    -
    ```
    Last login: Tue Apr 11 00:20:00 on ttys000
    jsy@jeongseong-yeob-ui-MacBookPro ~ % nslookup www.naver.com
    Server:         210.220.163.82
    Address:        210.220.163.82#53

    Non-authoritative answer:
    www.naver.com   canonical name = www.naver.com.nheos.com.
    Name:   www.naver.com.nheos.com
    Address: 223.130.200.104
    Name:   www.naver.com.nheos.com
    Address: 223.130.195.95

    jsy@jeongseong-yeob-ui-MacBookPro ~ %
    ```
    - 한국의 웹 서버에 대하여 nslookup 명령어를 사용 하기 위해 www.naver.com 을 넣어서 진행했고 ip address 는 223.130.200.104 또는 223.130.195.95 이다. 해당 주소를 주소창에 입력하면 naver 에 접속하게 된다.
2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe.

```
jsy@jeongseong-yeob-ui-MacBookPro ~ % nslookup -type=NS ox.ac.uk
Server:         210.220.163.82
Address:        210.220.163.82#53

Non-authoritative answer:
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.

Authoritative answers can be found from:
dns0.ox.ac.uk   internet address = 129.67.1.190
dns1.ox.ac.uk   internet address = 129.67.1.191
dns2.ox.ac.uk   internet address = 163.1.2.190
auth4.dns.ox.ac.uk      internet address = 45.33.127.156
auth5.dns.ox.ac.uk      internet address = 93.93.128.67
auth6.dns.ox.ac.uk      internet address = 185.24.221.32
auth4.dns.ox.ac.uk      has AAAA address 2600:3c00:e000:19::1
auth5.dns.ox.ac.uk      has AAAA address 2a00:1098:0:80:1000::10
auth6.dns.ox.ac.uk      has AAAA address 2a02:2770:11:0:21a:4aff:febe:759b
```

-
- 유럽의 옥스퍼드 대학 홈페이지에 nslookup 명령어에 www.ox.ac.kr 을 입력하여 DNS 서버를 확인하였다.

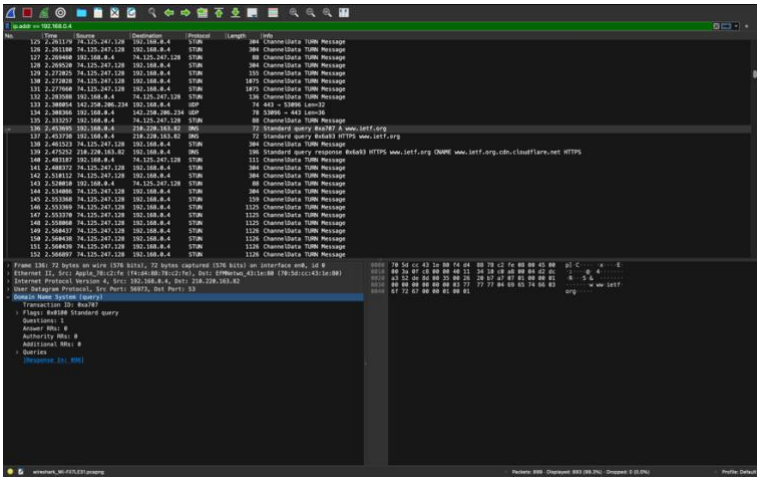
3. Run *nslookup* so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

```
Last login: Tue Apr 11 00:22:39 on ttys000
jsy@jeongseong-yeob-ui-MacBookPro ~ % nslookup ox.ac.uk mail.yahoo.com

;; connection timed out; no servers could be reached
```

-
- 맥북에서는 IP 주소를 확인할 수 없어서 윈도우로 진행하였다.

```
C:\Users\user>nslookup ox.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.
```

-
- Yahoo!의 메일 서버에 대해 query 를 한 경우 DNS 서버의 IP 주소는 119.161.8.11 이다.



4. Locate the DNS query and response messages. Are then sent over UDP or TCP?

```
> Frame 136: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface en0, id 0
> Ethernet II, Src: Apple_78:c2:fe (f4:d4:88:78:c2:fe), Dst: EFMNetwo_43:1e:80 (70:5d:cc:43:1e:80)
> Internet Protocol Version 4, Src: 192.168.0.4, Dst: 210.220.163.82
v User Datagram Protocol, Src Port: 56973, Dst Port: 53
    Source Port: 56973
    Destination Port: 53
    Length: 38
    Checksum: 0x20b7 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 6]
  > [Timestamps]
    UDP payload (30 bytes)
> Domain Name System (query)
```

-

- DNS query 와 response message 는 UDP 를 통해 보내졌다.

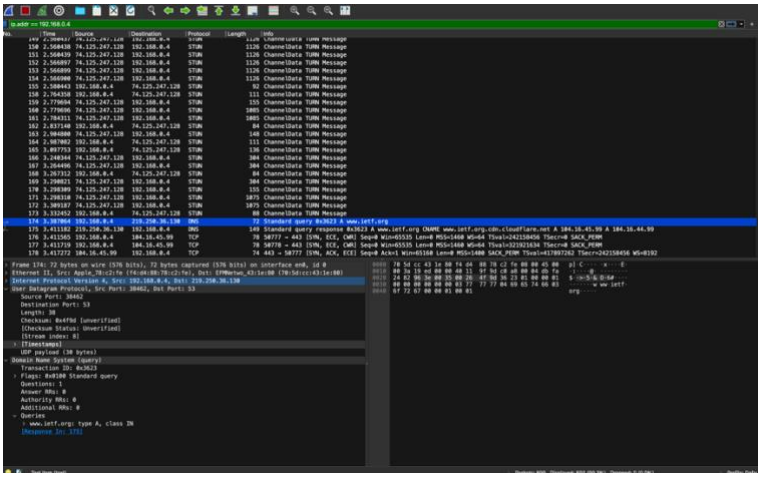
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
   - 위의 사진을 보면 destination port 는 53 이고 source port 는 56973 이다.
6. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?

```
jsy@jeongseong-yeob-ui-MacBookPro ~ % ipconfig getsummary en0
<dictionary> {
  BSSID : 70:5d:cc:43:1e:80
  IPv4 : <array> {
    0 : <dictionary> {
      Addresses : <array> {
        0 : 192.168.0.4
      }
      ChildServiceID : LINKLOCAL-en0
      ConfigMethod : DHCP
      DHCP : <dictionary> {
        LeaseExpirationTime : 04/11/2023 02:18:10
        LeaseStartTime : 04/11/2023 00:18:10
        Packet : op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0xf8031d31
secs = 0
ciaddr = 192.168.0.4
yiaddr = 192.168.0.4
siaddr = 0.0.0.0
giaddr = 0.0.0.0
chaddr = f4:d4:88:78:c2:fe
sname =
file =
options:
Options count is 7
dhcp_message_type (uint8): ACK 0x5
server_identifier (ip): 192.168.0.1
lease_time (uint32): 0x1c20
subnet_mask (ip): 255.255.255.0
router (ip_mult): {192.168.0.1}
domain_name_server (ip_mult): {210.220.163.82, 219.250.36.130}
```

-

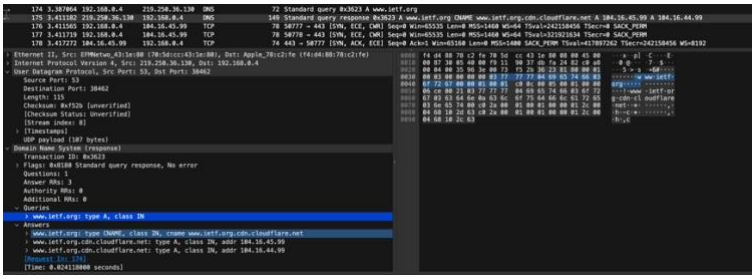
- DNS 는 210.220.163.82 이고 같은 address 를 사용하는 것을 볼 수 있다.

7. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



-
- query message type 은 "A" type 이다. 하지만 message 는 answers 을 가지고 있지 않다.

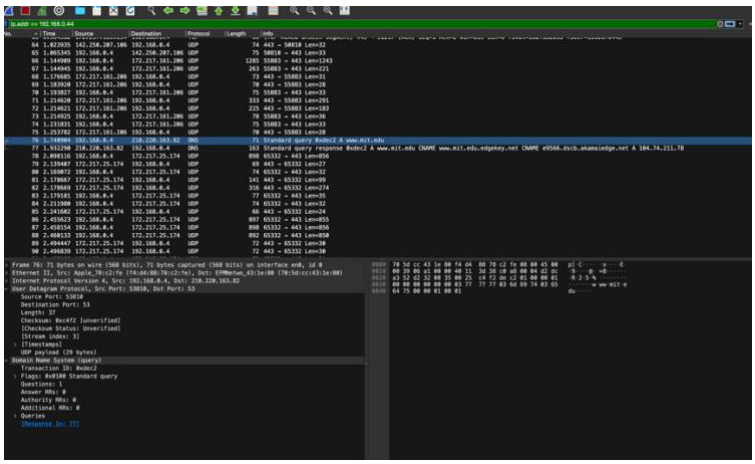
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?



-
- 3 개의 answer 을 제공하고 있으며 host name, address type, class, cname(IP Address) 등을 포함하고 있다.

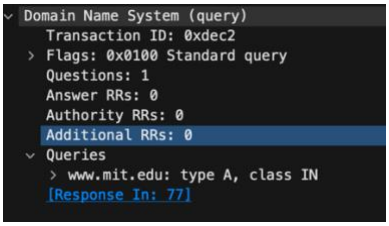
9. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
   - SYN 패킷 대상이 104.16.45.99 이고 DNS response message 에서의 주소가 웹 페이지 "A" 유형의 주소와 같다.
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?
    - 지난 http 에서 가져온 것과 다르게 사진에 대해 GET 이 일어나지 않으며 새로운 DNS query 들을 요청하지 않는다.

```
jsy@jeongseong-yeob-ui-MacBookPro ~ % nslookup www.mit.edu
Server:         210.220.163.82
Address:        210.220.163.82#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 104.74.211.78
```



```
jsy@jeongseong-yeob-ui-MacBookPro ~ % ipconfig getsummary en0
<dictionary> {
  BSSID : 70:5d:cc:43:1e:80
  IPv4 : <array> {
    0 : <dictionary> {
      Addresses : <array> {
        0 : 192.168.0.4
      }
      ChildServiceID : LINKLOCAL-en0
      ConfigMethod : DHCP
      DHCP : <dictionary> {
        LeaseExpirationTime : 04/11/2023 02:18:10
        LeaseStartTime : 04/11/2023 00:18:10
        Packet : op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 0xf8031d31
secs = 0
ciaddr = 192.168.0.4
yiaddr = 192.168.0.4
siaddr = 0.0.0.0
giaddr = 0.0.0.0
chaddr = f4:d4:88:78:c2:fe
sname =
file =
options:
Options count is 7
dhcp_message_type (uint8): ACK 0x5
server_identifier (ip): 192.168.0.1
lease_time (uint32): 0x1c20
subnet_mask (ip): 255.255.255.0
router (ip_mult): {192.168.0.1}
domain_name_server (ip_mult): {210.220.163.82, 219.250.36.130}
```

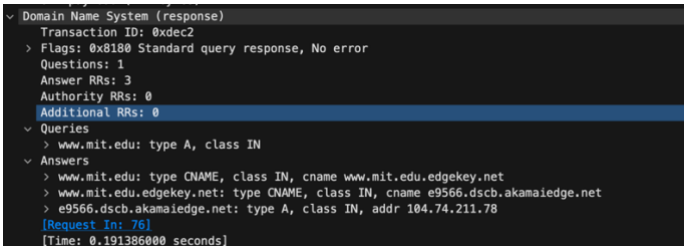
11. What is the destination port for the DNS query message? What is the source port of DNS response message?
    - Destination port 는 53 이고 source port 는 53810 이다.
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - 210.220.163.82 DNS 서버로 전송된다. 그리고 이것은 내 default local DNS server 와 같다.
13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?



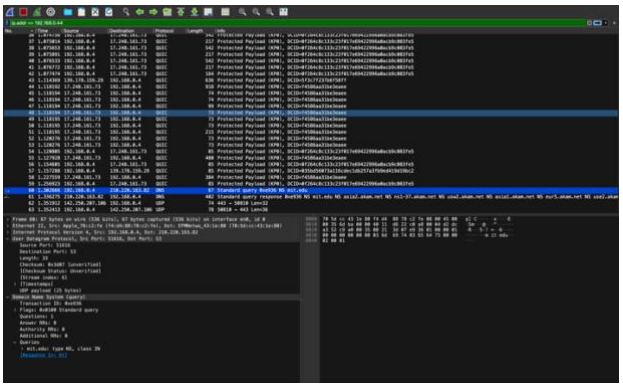
```
Domain Name System (query)
    Transaction ID: 0xdec2
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.mit.edu: type A, class IN
    [Response In: 77]
```

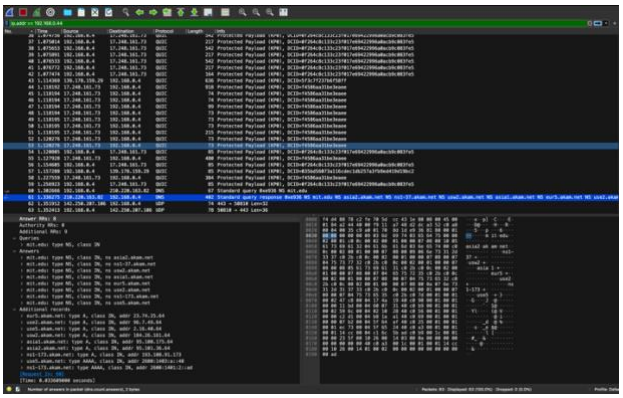
    -
    - DNS query 는 A 타입이고, question 하나를 가지지만 Answers 은 없다

14. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?



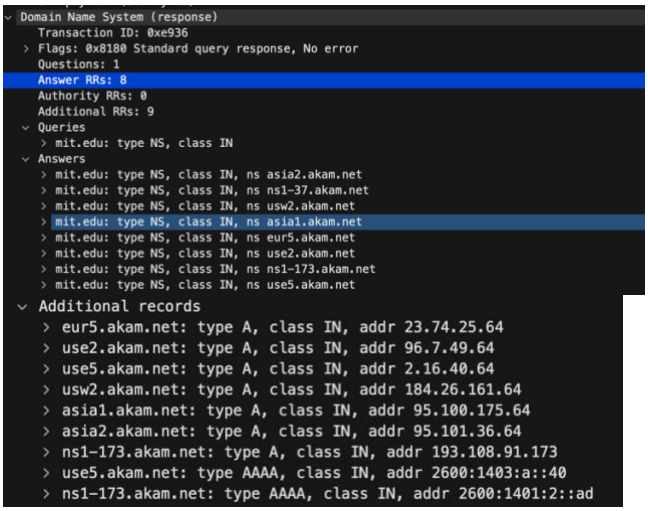
-
  - Response message 에서 answer 들은 3 개가 제공되고 각 answer 은 host name, type, class, cname(IP Address) 등을 포함하고 있다.
15. Provide a screenshot.
    - 사진은 위에서 사용하였다.(위의 사진 참고)





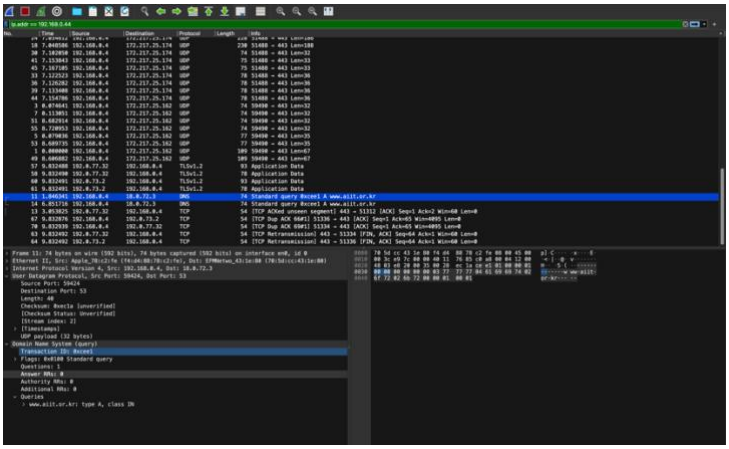
16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
    - DNS query message 는 210.220.163.82 로 보내고 이는 내 컴퓨터의 default local DNS server 주소와 같다.
17. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
    - 타입은 NS 이고 question 하나를 가지고 있지만 answer 는 포함하지 않는다.

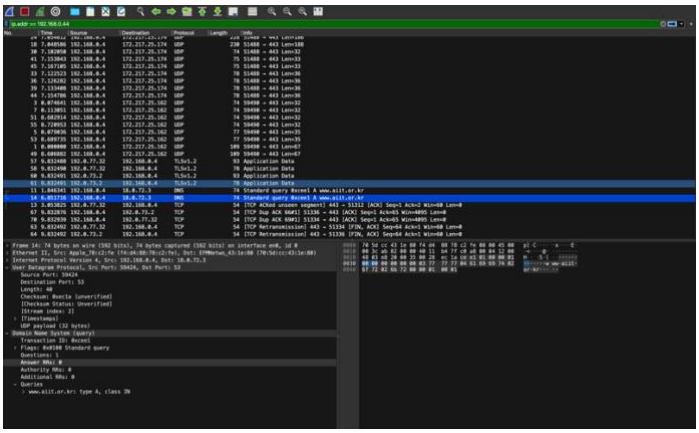
18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?



-
-
- Response message 에는 8 개의 answers 이 있으며 host name, type, class, ns 등을 포함하고 있고 아래 Additional records 에는 ns 에 대한 이름, type, class, IP address 를 포함하고 있다. 그러므로 이 response message 는 IP addresses 를 포함하고 있다.

19. Provide a screenshot.
    - 사진은 위에서 사용하였다. (위의 사진 참고)





20. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?

```
jsy@jeongseong-yeob-ui-MacBookPro ~ % nslookup bitsy.mit.edu
Server:         210.220.163.82
Address:        210.220.163.82#53

Non-authoritative answer:
Name:   bitsy.mit.edu
Address: 18.0.72.3

jsy@jeongseong-yeob-ui-MacBookPro ~ % ping bitsy.mit.edu
PING bitsy.mit.edu (18.0.72.3): 56 data bytes
64 bytes from 18.0.72.3: icmp_seq=0 ttl=37 time=256.879 ms
64 bytes from 18.0.72.3: icmp_seq=1 ttl=37 time=278.172 ms
64 bytes from 18.0.72.3: icmp_seq=2 ttl=37 time=298.917 ms
64 bytes from 18.0.72.3: icmp_seq=3 ttl=37 time=322.626 ms
^C
--- bitsy.mit.edu ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 256.879/289.149/322.626/24.382 ms
```

-
- DNS query message 의 destination 은 18.0.72.3 으로 bitsy.mit.edu 의 IP address 로 보내진다. 내 default local dns 가 아니다.

21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

```
Domain Name System (query)
    Transaction ID: 0xcee1
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.aiit.or.kr: type A, class IN
```

-
- 타입은 A type 이고 question 을 하나 가지고 있다. 하지만 Answer 은 없다.

22. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
    - DNS query message 는 존재하지만 response 는 존재하지 않는다. 그 이유는 터미널에서 nslookup 을 실행했을 때 받아온 것이 없기 때문이다.

```
jsy@jeongseong-yeob-ui-MacBookPro ~ % nslookup www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached

jsy@jeongseong-yeob-ui-MacBookPro ~ %
```

-
    - 터미널 결과를 보면 어느 서버에도 닿지 못했다고 하며 timed out 이 된다. 그래서 response 가 없다고 예상한다.

23. Provide a screenshot.
    - 사진은 위에서 사용하였다.(위의 사진 참고)

3. 결론 및 고찰(5줄 이상)

이번 과제를 통해서 wireshark를 통해 컴퓨터 네트워크 통신에 있어 패킷이 어떻게 사용되는지 또한 어떤 패킷이 어떤 역할을 하고 해당 내용은 무엇이 포함되어 제공되는지 알아보았다. 처음 써보는 프로그램과 배운지 얼마되지 않은 개념을 가지고 과제를 진행할 때는 어려운 점도 있었지만 차근차근 되짚어 보며 패킷이 가지고 있는 내용들을 확인할 수 있었고, 또한 macOS에서 진행한

wireshark가 주어진 예시와 약간씩 다르다 보니 따로 웹 서핑하며 찾아보았다. question#2에서 특정 페이지를 처음 들어갔을 때의 패킷과 다시 들어갔을 때 패킷이 다른데 결과가 달라진 것을 보고 당황했으나, 최근에 교수님께서 가르쳐 주신 캐시를 기억하여 사이트에 대한 캐시를 지우고 다시 처음부터 진행할 수 있었다. 마지막으로 DNS의 22번 문제에서 www.aiit.or.kr에서 bitsy.mit.edu의 서버에 접근할 때 도달하지 못하였는데 이 때 query response값도 받지 못하는 것이 의문이 들었다. 에러 메세지라도 받아올 줄 알았는데 없던 것을 보면 해당 페이지는 오류 출력에 있어 구현이 되지 않았거나 macOS 상에서 nslookup 명령어가 서버에 접근 못하면 못 받아오는 것으로 끝나게 하는 것인지 더 찾아보았고, 무조건 query response가 나타나는 것이 아님을 확인하였다.