

컴퓨터네트워크

Assignment1

강의 시간: 화5, 목6

교수님: 이혁준 교수님

학번: 2022202065

이름: 박나림

학과: 컴퓨터정보공학부

제출 일자: 2024년 04월 10일

1. Introduction

네트워크 프로토콜을 이해하기 위한 프로젝트로, Wireshark를 이용하여 진행한다.

Wireshark를 통해 패킷 캡처를 하고 이를 분석하는 것이 목표이다. 즉, 컴퓨터가 송신, 수신하는 모든 링크 레이어 프레임의 사본을 수신하고 이를 프로토콜 메시지와 함께 시각화 시키는 것을 공부하여 본다. 따라서 이러한 툴을 설치하는 것부터 시작하여 cmd창에서 자신의 컴퓨터의 IP를 확인하고, 이에 따른 문제풀이를 3과정에 걸쳐 진행한다.

첫번째는 자신의 IP를 확인하고 Wireshark를 실행해보며, 두번째로는 http에 대한 문제를 풀면서 공부해본다. 마지막으로 DNS에 대한 문제를 풀면서 네트워크 프로토콜을 이해할 수 있도록 한다.

2. 결과화면

-Question #1

cmd에서 IP화면을 캡처한 결과이다. 사용중인 Wi-Fi의 주소등의 정보가 나온다.

```
C:\Users\박나림>ipconfig

Windows IP 구성

무선 LAN 어댑터 로컬 영역 연결 * 1:

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

무선 LAN 어댑터 로컬 영역 연결 * 2:

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

이더넷 어댑터 VMware Network Adapter VMnet1:

    연결별 DNS 접미사 . . . . :
    링크-로컬 IPv6 주소 . . . . : fe80::8b72:7ae4:3c8f:a4f3%9
    IPv4 주소 . . . . . : 192.168.245.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

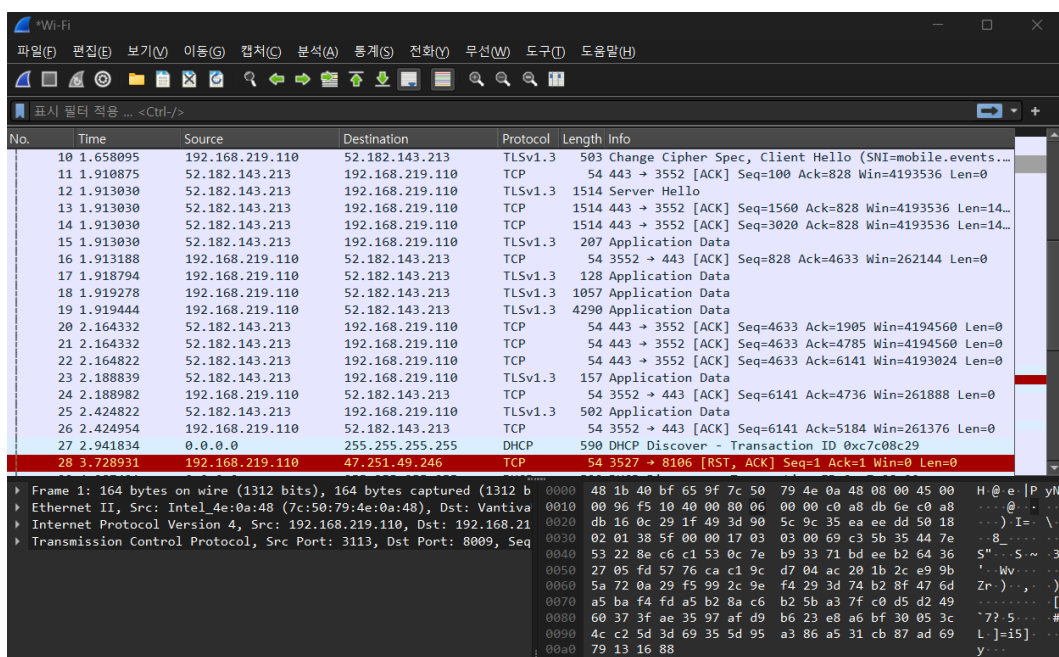
이더넷 어댑터 VMware Network Adapter VMnet8:

    연결별 DNS 접미사 . . . . :
    링크-로컬 IPv6 주소 . . . . : fe80::ada3:19ab:c078:9116%16
    IPv4 주소 . . . . . : 192.168.59.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

무선 LAN 어댑터 Wi-Fi:

    연결별 DNS 접미사 . . . . : Davolink
    링크-로컬 IPv6 주소 . . . . : fe80::5eae:debb:ca3b:66b3%8
    IPv4 주소 . . . . . : 192.168.219.110
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 192.168.219.1
```

PC에서 동작중인 Wireshark화면을 캡처한 결과이다. (Wi-Fi 사용)



-Question #2

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

위 주소에 접속한 결과는 아래와 같다. (1~7번 문제)

167	11.408766	192.168.219.110	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
176	11.614932	128.119.245.12	192.168.219.110	HTTP	540 HTTP/1.1 200 OK (text/html)
181	11.651010	192.168.219.110	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
201	11.858832	128.119.245.12	192.168.219.110	HTTP	538 HTTP/1.1 404 Not Found (text/html)

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

-browser와 server 모두 아래와 같이 HTTP 1.1이다.

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 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=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko-KR,ko;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/2]
[Response in frame: 176]
[Next request in frame: 181]
```

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
Date: Sun, 07 Apr 2024 06:17:46 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 07 Apr 2024 05:59:02 GMT\r\n
ETag: "80-6157b62c52132"\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 1/2]
[Time since request: 0.206166000 seconds]
[Request in frame: 167]
[Next request in frame: 181]
[Next response in frame: 201]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

2. What languages (if any) does your browser indicate that it can accept to the server?

-Accept Language: ko-KR, ko; q=0.9

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 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=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko-KR,ko;q=0.9\r\n
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

-아래에 나와있는 Src는 컴퓨터 IP주소로, 192.168.219.110이다. Dst인 gaia.cs.umass.edu server의 IP주소는 128.119.245.12이다.

```
▶ Frame 167: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits)
▶ Ethernet II, Src: Intel_4e:0a:48 (7c:50:79:4e:0a:48), Dst: GongjinElect_
▶ Internet Protocol Version 4, Src: 192.168.219.110, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 3587, Dst Port: 80, Seq: 1, Ack
▶ Hypertext Transfer Protocol
```

4. What is the status code returned from the server to your browser?

-status code는 200인걸 볼 수 있다.

```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
```

5. When was the HTML file that you are retrieving last modified at the server?

-server의 Last Modified는 Sun, 07 Apr 2024 05:59:02 GMT이다.

```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sun, 07 Apr 2024 06:17:46 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips P
    Last-Modified: Sun, 07 Apr 2024 05:59:02 GMT\r\n
```

6. How many bytes of content are being returned to your browser?

-128byte이다.

```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sun, 07 Apr 2024 06:17
    Server: Apache/2.4.6 (CentOS
    Last-Modified: Sun, 07 Apr 2
    ETag: "80-6157b62c52132"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 128\r\n
```

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.

-패킷창에 나타나는 데이터 내의 헤더가 없기 때문에 보이지 않는다.

.....
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

위 주소에 접속한 결과는 아래와 같다. (8~11번 문제)

195	12.073246	192.168.219.110	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
198	12.432353	128.119.245.12	192.168.219.110	HTTP	784 HTTP/1.1 200 OK (text/html)
202	12.464467	192.168.219.110	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
233	12.670459	128.119.245.12	192.168.219.110	HTTP	538 HTTP/1.1 404 Not Found (text/html)

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?

-첫번째 GET에서 IF-MODIFIED-SINCE line은 보이지 않는다.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

-server에 응답을 보면, 아래와 같이 파일 내용을 반환한 것을 볼 수 있다. html파일의 코드가 나타난다.

```
▼ 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. 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?

-페이지를 새로고침하여 두번째 HTTP GET을 확인한 결과이다. IF_MODIFIED_SINCE line이 생긴 것을 볼 수 있다. Sun, 07 Apr 2024 05:59:02 GMT로 나타나는데, 이 정보는 아까 5번문제에서 확인한 결과와 같다. 즉, 이전 요청에서 파일을 마지막으로 수정한 날짜가 보이는 것이다.

247	25.886415	192.168.219.110	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
252	25.914748	192.168.219.110	211.115.106.80	HTTP	443	GET /jk?c=62&p=+Je+J6Ox040sNitYNdY65BzcLuMdGX1L5RSm3qI4ebM=&k=1 HTTP/1.1
254	25.926098	211.115.106.80	192.168.219.110	HTTP	415	HTTP/1.1 200 OK
282	26.748321	128.119.245.12	192.168.219.110	HTTP	784	HTTP/1.1 200 OK (text/html)
287	26.766074	192.168.219.110	211.115.106.80	HTTP	487	GET /jk?c=62&p=+Je+J6Ox040sNitYNdY65BzcLuMdGX1L5RSm3qI4ebM=&k=1 HTTP/1.1
290	26.775065	211.115.106.80	192.168.219.110	HTTP	415	HTTP/1.1 200 OK
291	26.780507	192.168.219.110	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
307	26.984868	128.119.245.12	192.168.219.110	HTTP	538	HTTP/1.1 404 Not Found (text/html)
345	41.784888	192.168.219.110	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
348	42.065952	128.119.245.12	192.168.219.110	HTTP	294	HTTP/1.1 304 Not Modified

```

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
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9\r\n
  If-None-Match: "173-6157b62c51962"\r\n
  If-Modified-Since: Sun, 07 Apr 2024 05:59:02 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: 348]

```

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.

-Status Code: 304, Response Phrase: Not Modified로 응답된 것을 볼 수 있다. 이 파일의 마지막 수정 날짜는 변경되지 않는다는 뜻이다. 또한 두번째 HTTP GET에서는 html 파일의 내용이 반환되지 않는다. 여러 번 다운로드 해도 GET 요청에 IN-MODIFIED-SINCE 필드가 포함되어 있기 때문에, 전체 복사본은 서버에서 한번만 전송되기 때문이다. 따라서 첫번째 GET요청에서 파일의 내용이 한번 반환되고, 두번째부터 반환되지 않는 것이다.

```

Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      [HTTP/1.1 304 Not Modified\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified

```

.....
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

위 주소에 접속한 결과는 아래와 같다. (12~15번 문제)

254	20.499933	192.168.219.110	128.119.245.12	HTTP	526 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
261	20.709073	128.119.245.12	192.168.219.110	HTTP	535 HTTP/1.1 200 OK (text/html)
268	20.777852	192.168.219.110	128.119.245.12	HTTP	472 GET /favicon.ico HTTP/1.1
298	20.982001	128.119.245.12	192.168.219.110	HTTP	538 HTTP/1.1 404 Not Found (text/html)

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?

-GET요청 메시지는 1번, packet 번호는 254이다.

254 20.499933

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

-GET 요청에 대한 응답과 관련된 packet 번호는 261이다.

261 20.709073

14. What is the status code and phrase in the response?

-Status Code: 200, Response Phrase: OK로 표시된다.

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

-필요한 TCP Segments는 4개로, #258(1460), #259(1460), #260(1460), #261(481)인 것을 볼 수 있다.

```
[4 Reassembled TCP Segments (4861 bytes): #258(1460), #259(1460), #260(1460), #261(481)]
[Frame: 258, payload: 0-1459 (1460 bytes)]
[Frame: 259, payload: 1460-2919 (1460 bytes)]
[Frame: 260, payload: 2920-4379 (1460 bytes)]
[Frame: 261, payload: 4380-4860 (481 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4861]
[Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446174653a2053756
```


.....

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

위 주소에 접속한 결과는 아래와 같다. (16~17번 문제)

165	8.478861	192.168.219.110	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
169	8.811135	128.119.245.12	192.168.219.110	HTTP	1355	HTTP/1.1 200 OK (text/html)
172	8.818636	192.168.219.110	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
176	9.023881	128.119.245.12	192.168.219.110	HTTP	745	HTTP/1.1 200 OK (PNG)
190	9.413911	192.168.219.110	211.115.106.72	HTTP	443	GET /jk?d=62&p=+Je+J6Ox040sNitYNdY65BzclUMdGX1L5RSm3qI4ebM=&k=1 HTTP/1.1
192	9.425099	211.115.106.72	192.168.219.110	HTTP	415	HTTP/1.1 200 OK
194	9.471217	192.168.219.110	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
203	10.383640	178.79.137.164	192.168.219.110	HTTP	225	HTTP/1.1 301 Moved Permanently
706	16.908783	192.168.219.110	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
709	17.305012	128.119.245.12	192.168.219.110	HTTP	539	HTTP/1.1 404 Not Found (text/html)

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

-주소, png, jpg를 가져오는 3회의 GET 요청으로, 순서대로 128.119.245.12, 128.119.245.12, 178.79.137.164이다.

165	8.478861	192.168.219.110	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
169	8.811135	128.119.245.12	192.168.219.110	HTTP	1355	HTTP/1.1 200 OK (text/html)
172	8.818636	192.168.219.110	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
176	9.023881	128.119.245.12	192.168.219.110	HTTP	745	HTTP/1.1 200 OK (PNG)
190	9.413911	192.168.219.110	211.115.106.72	HTTP	443	GET /jk?d=62&p=+Je+J6Ox040sNitYNdY65BzclUMdGX1L5RSm3qI
192	9.425099	211.115.106.72	192.168.219.110	HTTP	415	HTTP/1.1 200 OK
194	9.471217	192.168.219.110	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1

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.

-처음 브라우저 주소에 접속하고 순서대로 이미지만 가져온 것이 보이기 때문에, 따로 주소를 한 번 더 접속해서 두 웹사이트에서 병렬로 다운로드하지 않은 걸 알 수 있다. 첫번째로 pearson.png를 가져오고 두번째로 8E_cover_small.jpg를 가져왔다.

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

위 주소에 접속한 결과는 아래와 같다. (18~19번 문제)

275	19.711771	192.168.219.110	128.119.245.12	HTTP	542 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
277	20.107632	128.119.245.12	192.168.219.110	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
396	30.743999	192.168.219.110	128.119.245.12	HTTP	627 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
399	30.967661	128.119.245.12	192.168.219.110	HTTP	544 HTTP/1.1 200 OK (text/html)

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

-Status Code: 401, Response Phrase: Unauthorized로 나타난다.

- ▼ Hypertext Transfer Protocol
 - ▼ HTTP/1.1 401 Unauthorized\r\n
 - ▶ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]Response Version: HTTP/1.1Status Code: 401[Status Code Description: Unauthorized]Response Phrase: Unauthorized

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

-로그인을 하고 나서 나타난 두번째 GET을 보면 아래와 같이 새로운 필드가 나타난다.

Authorization: Basic d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcms=wrWn

Credentials: wireshark-students:network

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5z\r\n
      Credentials: wireshark-students:network
```

-Question #3

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

- naver 서버를 접속했을 때 223.130.200.236 / 223.130.192.248 / 223.130.192.247 / 223.130.200.219와 같이 IP주소가 나타난다.

```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\박나림>nslookup www.naver.com
서버:      acns.uplus.co.kr
Address:  1.214.68.2

권한 없는 응답:
이름:      www.naver.com.nheos.com
Addresses: 223.130.200.236
           223.130.192.248
           223.130.192.247
           223.130.200.219
Aliases:   www.naver.com
```

2. Run nslookup to determine the authoritative DNS servers for a university in Europe.

-primary.dns.cam.ac.uk로 나온다. (처음에 기존처럼 cmd를 실행했다가 결과가 나오지 않아서 관리자모드로 cmd를 실행하니 두번째처럼 결과가 나왔다.)

```
C:\Users\박나림>nslookup -type=NS www.cam.ac.uk
서버:      acns.bora.net
Address:  1.214.68.2

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

```
C:\Windows\System32>nslookup -type=NS www.cam.ac.uk
서버:      acns.uplus.co.kr
Address:  1.214.68.2

cam.ac.uk
    primary name server = primary.dns.cam.ac.uk
    responsible mail addr = hostmaster.cam.ac.uk
    serial = 1712733151
    refresh = 1800 (30 mins)
    retry = 900 (15 mins)
    expire = 604800 (7 days)
    default TTL = 3600 (1 hour)
```

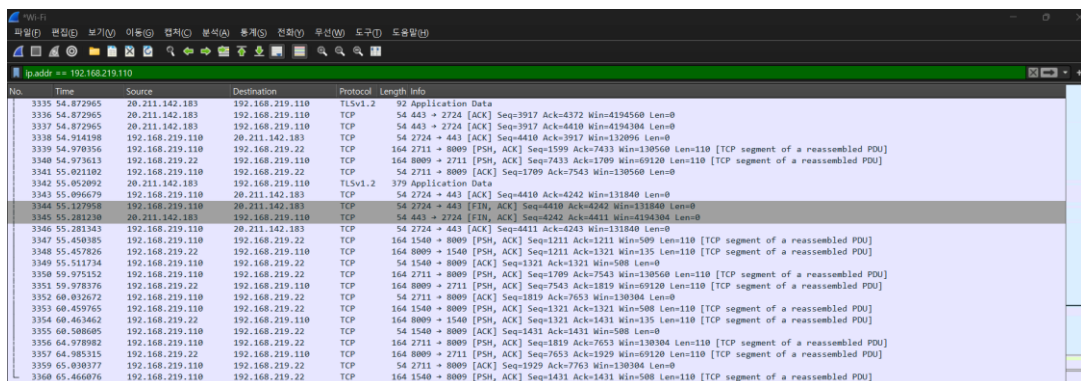
3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. What is its IP address?

-그전에서 얻은 DNS 서버를 Yahoo!용 메일 서버에 대해 쿼리하면 다음과 같이 DNS 서버의 ip주소가 180.222.116.11로 나오는 것을 볼 수 있다.

```
C:\Users\박나림>nslookup www.cam.ac.uk mail.yahoo.com
DNS request timed out.
    timeout was 2 seconds.
서버:      Unknown
Address:   180.222.116.11

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.
```

(4~10번 문제) ipconfig를 사용하여 host의 DNS 캐시를 비운 후, 브라우저의 캐시까지 비운다. 그 다음 Wireshark에서 ip.addr == 192.168.219.110(컴퓨터 ip)를 입력한다.



그 상태에서 http://www.ietf.org 를 방문한 후 패킷 캡처 중지, DNS 필터로 검색한 결과이다.

No.	Time	Source	Destination	Protocol	Length	Info
1631	41.689820	192.168.219.110	192.168.219.110	DNS	152	Standard query response 0x4a4d HTTPS optimizationguide-pa.googleapis.com SOA ns1.google.com
1811	50.496534	192.168.219.110	192.168.219.110	DNS	72	Standard query 0x5822 A www.ietf.org
1812	50.496872	192.168.219.110	192.168.219.110	DNS	72	Standard query 0x8fa5 HTTPS www.ietf.org
1815	50.501073	192.168.219.110	192.168.219.110	DNS	104	Standard query response 0x5822 A www.ietf.org A 104.16.45.99 A 104.16.44.99
1817	50.504115	192.168.219.110	192.168.219.110	DNS	72	Standard query 0xe4ca A www.ietf.org
1818	50.504259	192.168.219.110	192.168.219.110	DNS	72	Standard query 0x8818 HTTPS www.ietf.org
1819	50.504330	192.168.219.110	192.168.219.110	DNS	145	Standard query response 0x8fa5 HTTPS www.ietf.org HTTPS
1820	50.508064	192.168.219.110	192.168.219.110	DNS	104	Standard query response 0xe4ca A www.ietf.org A 104.16.44.99 A 104.16.45.99
1821	50.511943	192.168.219.110	192.168.219.110	DNS	145	Standard query response 0x8818 HTTPS www.ietf.org HTTPS
1856	50.586998	192.168.219.110	192.168.219.110	DNS	83	Standard query 0xff20 A safebrowsing.google.com
1857	50.587130	192.168.219.110	192.168.219.110	DNS	83	Standard query 0x5b33 HTTPS safebrowsing.google.com
1858	50.591707	192.168.219.110	192.168.219.110	DNS	152	Standard query response 0x5b35 HTTPS safebrowsing.google.com CNAME sb.l.google.com SOA ns1.google.com
1859	50.591707	192.168.219.110	192.168.219.110	DNS	118	Standard query response 0xff20 A safebrowsing.google.com CNAME sb.l.google.com A 172.217.31.14
1944	50.824556	192.168.219.110	192.168.219.110	DNS	75	Standard query 0x8fa9 A static.ietf.org
1945	50.824746	192.168.219.110	192.168.219.110	DNS	75	Standard query 0xae77 HTTPS static.ietf.org
1948	50.832326	192.168.219.110	192.168.219.110	DNS	107	Standard query response 0x8fa9 A static.ietf.org A 104.16.45.99 A 104.16.44.99
1950	50.835064	192.168.219.110	192.168.219.110	DNS	148	Standard query response 0xae77 HTTPS static.ietf.org HTTPS
2194	50.957662	192.168.219.110	192.168.219.110	DNS	78	Standard query 0xb9ba A analytics.ietf.org
2195	50.957848	192.168.219.110	192.168.219.110	DNS	78	Standard query 0x2794 HTTPS analytics.ietf.org
2198	50.970112	192.168.219.110	192.168.219.110	DNS	151	Standard query response 0x2794 HTTPS analytics.ietf.org HTTPS
2205	50.985790	192.168.219.110	192.168.219.110	DNS	84	Standard query 0x3735 A translate.googleapis.com
2206	50.985975	192.168.219.110	192.168.219.110	DNS	84	Standard query 0xc8d8 HTTPS translate.googleapis.com
2208	50.992218	192.168.219.110	192.168.219.110	DNS	100	Standard query response 0x3735 A translate.googleapis.com A 142.251.220.42
2209	50.992218	192.168.219.110	192.168.219.110	DNS	141	Standard query response 0xc8d8 HTTPS translate.googleapis.com SOA ns1.google.com
2396	51.023036	192.168.219.110	192.168.219.110	DNS	110	Standard query response 0xb9ba A analytics.ietf.org A 104.16.45.99 A 104.16.44.99
3290	52.837406	192.168.219.110	192.168.219.110	DNS	91	Standard query 0x8a19 A settings-win.data.microsoft.com

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

- 위와 같이 DNS query와 response 메시지를 눌러서 보면, 아래처럼 UDP(User Datagram Protocol)로 전송된 것을 볼 수 있다.

```
Internet Protocol Version 4, Src: 192.168.219.110, Dst: 1.214.68.2
User Datagram Protocol, Src Port: 49664, Dst Port: 53
```

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

-destination port는 53, Source Port는 49664로 나타난다.

```
Internet Protocol Version 4, Src: 192.168.219.110, Dst: 1.214.68.2
User Datagram Protocol, Src Port: 49664, Dst Port: 53
Source Port: 49664
Destination Port: 53
Length: 38
```

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?

-DNS query는 1.214.68.2로 전송되었다. ipconfig /all을 통해 확인한 결과에서도 마찬가지로 1.214.68.2로 동일하다.

```
192.168.219.110 1.214.68.2 DNS 72 Standard query 0x5822 A www.ietf.org
```

```
무선 LAN 어댑터 Wi-Fi:
연결 별 DNS 접미사 . . . . : Davolink
설명 . . . . . : Intel(R) Wi-Fi 6E AX210 160MHz
물리적 주소 . . . . . : 7C-50-79-4E-0A-48
DHCP 사용 . . . . . : 예
자동 구성 사용 . . . . . : 예
링크-로컬 IPv6 주소 . . . . : fe80::5eae:debb:ca3b:66b3%8(기본 설정)
IPv4 주소 . . . . . : 192.168.219.110(기본 설정)
서브넷 마스크 . . . . . : 255.255.255.0
임대 시작 날짜 . . . . . : 2024년 4월 10일 수요일 오후 4:00:39
임대 만료 날짜 . . . . . : 2024년 4월 11일 목요일 오후 4:00:39
기본 게이트웨이 . . . . . : 192.168.219.1
DHCP 서버 . . . . . : 192.168.219.1
DHCPv6 IAID . . . . . : 92033145
DHCPv6 클라이언트 DUID . . . : 00-01-00-01-29-44-9A-C6-7C-50-79-4E-0A-48
DNS 서버 . . . . . : 1.214.68.2
```

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

-쿼리 메시지는 A type으로 나오고, 답변은 따로 포함되어 있지 않은 것을 볼 수 있다.

```
▼ Domain Name System (query)
  Transaction ID: 0x5822
  ▶ 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: 1815]
```

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

-응답 메시지에 관한 정보를 보면, 답변은 2개가 제공된 것을 볼 수 있다. 각 답변은 해당 사이트의 주소, type, class, addr를 포함하며 더 자세히는 Name, Type, Class, Time to live, Data length, Address가 있다.

```
1.214.68.2      192.168.219.110  DNS      104 Standard query response 0x5822 A www.ietf.org A 104.16.45.99 A 104.16.44.99
```

```
▼ Domain Name System (response)
  Transaction ID: 0x5822
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 2
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▶ www.ietf.org: type A, class IN
```

```
▼ Answers
  ▼ www.ietf.org: type A, class IN, addr 104.16.45.99
    Name: www.ietf.org
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 130 (2 minutes, 10 seconds)
    Data length: 4
    Address: 104.16.45.99
  ▼ www.ietf.org: type A, class IN, addr 104.16.44.99
    Name: www.ietf.org
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 130 (2 minutes, 10 seconds)
    Data length: 4
    Address: 104.16.44.99
  [Request In: 1811]
  [Time: 0.004539000 seconds]
```

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 packet의 대상 IP 주소는 104.16.45.99, 104.16.44.99로, 이는 DNS 응답 메시지에서 제공된 IP 주소와 동일한 주소이다.

```

▼ Answers
  ▶ www.ietf.org: type A, class IN, addr 104.16.45.99
  ▶ www.ietf.org: type A, class IN, addr 104.16.44.99
  
```

10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

-host는 이미지를 검색하기 전에 새로운 DNS 쿼리를 발행한다. 해당 쿼리가 이루어질 때까지 페이지에서는 그 이미지가 나타나지 않게 되는 것이다.

.....

(11~15번 문제) nslookup www.mit.edu로 패킷캡처를 수행한 결과이다.

795	76.054554	192.168.219.110	1.214.68.2	DNS	71 Standard query 0x0004 A www.mit.edu
800	77.821765	1.214.68.2	192.168.219.110	DNS	160 Standard query response 0x0004 A www.mit.edu
801	77.830487	192.168.219.110	1.214.68.2	DNS	71 Standard query 0x0005 AAAA www.mit.edu
802	77.847420	1.214.68.2	192.168.219.110	DNS	200 Standard query response 0x0005 AAAA www.mit.edu
815	83.420463	192.168.219.110	1.214.68.2	DNS	74 Standard query 0x3928 A gms.ahnlab.com
816	83.425542	1.214.68.2	192.168.219.110	DNS	112 Standard query response 0x3928 A gms.ahnlab.com

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

-쿼리 메시지의 destination port는 53, 응답 메시지의 source port는 53으로 동일하다. 응답 메시지가 53이니까 쿼리의 도착도 53으로 똑같은 것이다.

```

▼ User Datagram Protocol, Src Port: 60445, Dst Port: 53
  Source Port: 60445
  Destination Port: 53
  Length: 37
  Checksum: 0xe225 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 18]
  ▶ [Timestamps]
  UDP payload (29 bytes)
  ▶ Domain Name System (query)
  
```

```

▼ User Datagram Protocol, Src Port: 53, Dst Port: 60445
  Source Port: 53
  Destination Port: 60445
  Length: 126
  Checksum: 0xfc0d [unverified]
  [Checksum Status: Unverified]
  [Stream index: 18]
  ▶ [Timestamps]
  UDP payload (118 bytes)
  ▶ Domain Name System (response)
  
```

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

-DNS query 메시지는 1.214.68.2로 전송되며, 이는 ipconfig /all에서 확인한 DNS 서버 IP 주소와 같다는 것을 알 수 있다.

```
▶ Internet Protocol Version 4, Src: 192.168.219.110, Dst: 1.214.68.2
▶ User Datagram Protocol, Src Port: 60445, Dst Port: 53
▶ Domain Name System (query)
```

```
무선 LAN 어댑터 Wi-Fi:
연결별 DNS 접미사 . . . . : Davolink
설명 . . . . . : Intel(R) Wi-Fi 6E AX210 160MHz
물리적 주소 . . . . . : 7C-50-79-4E-0A-48
DHCP 사용 . . . . . : 예
자동 구성 사용 . . . . . : 예
링크-로컬 IPv6 주소 . . . . : fe80::5eae:debb:ca3b:66b3%8(기본 설정)
IPv4 주소 . . . . . : 192.168.219.110(기본 설정)
서브넷 마스크 . . . . . : 255.255.255.0
임대 시작 날짜 . . . . . : 2024년 4월 10일 수요일 오후 4:00:39
임대 만료 날짜 . . . . . : 2024년 4월 11일 목요일 오후 4:00:39
기본 게이트웨이 . . . . . : 192.168.219.1
DHCP 서버 . . . . . : 192.168.219.1
DHCPv6 IAID . . . . . : 92033145
DHCPv6 클라이언트 DUID . . : 00-01-00-01-29-44-9A-C6-7C-50-79-4E-0A-48
DNS 서버 . . . . . : 1.214.68.2
```

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

-DNS query 메시지의 type은 A이며, 답변은 포함하지 않는다.

```
▼ Queries
  ▼ www.mit.edu: type A, class IN
    Name: www.mit.edu
    [Name Length: 11]
    [Label Count: 3]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    [Response To: 800]
```

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

-DNS response 메시지는 3개의 답변을 포함하며, 각각 주소, type, class, cname 등을 포함한다.


```
▼ Domain Name System (response)
  Transaction ID: 0x0004
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 3
  Authority RRs: 0
  Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▶ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
    ▶ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
    ▶ e9566.dscb.akamaiedge.net: type A, class IN, addr 104.75.6.149
  [Request In: 795]
  [Time: 1.767211000 seconds]
```

15. Provide a screenshot.

-위와 같다.

(16~19번 문제) nslookup -type=NS mit.edu 수행한 결과이다.

192.168.219.110	1.214.68.2	DNS	67 Standard query 0x0003 NS mit.edu
1.214.68.2	192.168.219.110	DNS	234 Standard query response 0x0003 NS mit.edu

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

-위 결과를 보면 쿼리 메시지가 1.214.68.2로 전송된 것을 볼 수 있다. 이는 기본 로컬 DNS 서버의 IP주소와 같다.

DNS 서버 : 1.214.68.2

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

-DNS query 메시지의 type은 NS, 답변은 포함되어 있지 않다.

```
▼ Domain Name System (query)
  Transaction ID: 0x0003
  ▶ 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 (2) (authoritative Name Server)
      Class: IN (0x0001)
  [Response In: 60]
```

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 nameservers?

-use2.akam.net, eur5.akam.net, asia2.akam.net...등 아래와 같은 name 서버를 제공한다. IP 주소는 제공하지 않는다.

```

▼ Answers
  ▶ mit.edu: type NS, class IN, ns use2.akam.net
  ▶ mit.edu: type NS, class IN, ns eur5.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 ns1-37.akam.net
  ▶ mit.edu: type NS, class IN, ns use5.akam.net
  ▶ mit.edu: type NS, class IN, ns ns1-173.akam.net
[Request Id: 56]

```

19. Provide a screenshot.

-위와 같다.

(20~23번 문제) nslookup www.aiit.or.kr bitsy.mit.edu 를 수행한 결과이다.

192.168.219.110	1.214.68.2	DNS	73 Standard query 0x535d A bitsy.mit.edu
192.168.219.110	61.41.153.2	DNS	73 Standard query 0x535d A bitsy.mit.edu
1.214.68.2	192.168.219.110	DNS	89 Standard query response 0x535d A bitsy.mit.edu A 18.0.72.3
192.168.219.110	18.0.72.3	DNS	82 Standard query 0x0001 PTR 3.72.0.18.in-addr.arpa
61.41.153.2	192.168.219.110	DNS	89 Standard query response 0x535d A bitsy.mit.edu A 18.0.72.3
192.168.219.110	18.0.72.3	DNS	83 Standard query 0x0002 A www.aiit.or.kr.Davolink
192.168.219.110	18.0.72.3	DNS	83 Standard query 0x0003 AAAA www.aiit.or.kr.Davolink
192.168.219.110	18.0.72.3	DNS	74 Standard query 0x0004 A www.aiit.or.kr
192.168.219.110	18.0.72.3	DNS	74 Standard query 0x0005 AAAA www.aiit.or.kr

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?

-DNS query 메시지의 IP 주소는 18.0.72.3이고, 기본 로컬 DNS 서버의 IP주소는 1.124.68.2로 다르다. 18.0.72.3은 접속한 사이트의 IP주소에 해당한다.

192.168.219.110	18.0.72.3	DNS	74 Standard query 0x0004 A www.aiit.or.kr
192.168.219.110	18.0.72.3	DNS	74 Standard query 0x0005 AAAA www.aiit.or.kr

DNS 서버 : 1.214.68.2

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

-DNS query 메시지는 type A이다. 해당 메시지에는 답변이 포함되어 있지 않다.

```
▼ Queries
  ▼ www.aiit.or.kr: type A, class IN
    Name: www.aiit.or.kr
    [Name Length: 14]
    [Label Count: 4]
    Type: A (1) (Host Address)
    Class: IN (0x0001)
```

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

-DNS response 메시지에 하나의 답변이 제공된다. 주소, 타입, class, time to live, data length 등이 포함된다.

```
▼ Domain Name System (response)
  Transaction ID: 0x535d
  ▶ Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  ▶ Queries
  ▼ Answers
    ▶ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
      [Request In: 134]
      [Time: 0.241487000 seconds]

▼ Answers
  ▼ bitsy.mit.edu: type A, class IN, addr 18.0.72.3
    Name: bitsy.mit.edu
    Type: A (1) (Host Address)
    Class: IN (0x0001)
    Time to live: 1800 (30 minutes)
    Data length: 4
    Address: 18.0.72.3
```

23. Provide a screenshot.

-위와 같다.

3. 결론 및 고찰

프로젝트를 진행하면서, 여러 시행착오를 겪었다. 이번에 Wi-Fi 무선랜 환경에서 진행을 하였는데, 패킷 캡처를 할 때 링크가 제대로 나타나지 않았다. 이에 대한 방법들을 찾아보다 이더넷과 같이 유선랜으로 하는 방법을 생각해 보게 되었다. 하지만 이더넷을 통해서 패킷 캡처를 진행하여도 똑같이 링크가 제대로 뜨지 않았다. 그래서 네트워크 문제가 아니라 크롬 브라우저 상의 문제라고 짐작하였고, 캐시 삭제와 게스트모드로 진행하니 무사히 패킷 캡처가 정상적인 링크로 뜰 수 있게 되었다.

또한 문제 풀이를 진행하면서 어떤 정보가 어느 위치에 속해 있는지 파악하는데 시간이 걸렸던 것 같다. 계속 문제를 풀면서 이에 대해 익숙해졌고, 분석하는 방법을 더 잘 익힐 수 있었다.

이번 프로젝트를 통해 네트워크 프로토콜에 대해 다양하게 공부해보면서, IP주소나 DNS 서버 등에서 서로 패킷들을 수신, 송신하는 과정들을 더 잘 이해할 수 있었다.