Homework #1

1. **This elementary problem begins to explore propagation delay and transmission delay, two central concepts in data networking. Consider two hosts, A and B, connected by a single link of rate R bps. Suppose that the two hosts are separated by m meters, and suppose the propagation speed along the link is s meters/sec. Host A is to send a packet of size L bits to Host B.**

    a. **Ignoring processing and queueing delays, obtain an expression for the end-to-end delay, in terms of m, s, L, and R.**

       Ans)

       $$d = d_{prop} + d_{trans} = \frac{m}{s} \, sec + \frac{L}{R} sec$$

    b. **Suppose d_{prop} is greater than d_{trans}. At time $t=d_{trans}$, where is the first bit of the packet?**

       Ans)

       In link and has not reached host B.

    c. **Suppose d_{prop} is less than d_{trans}. At time $t=d_{trans}$, where is the first bit of the packet?**

       At host B

    d. **Suppose $s=2.5*10^8$, $L=150$bits, and $R=128$kbps. Find the distance m so that d_{prop} equals d_{trans}.**

       Ans)

       $$d_{prop} = \frac{m}{s} = d_{trans} = \frac{L}{R} \qquad \therefore \frac{m}{s} = \frac{L}{R}$$

       $$\frac{m}{2.5*10^8} = \frac{150}{128*10^3}, \qquad \therefore m = 292.97km$$

2. **Suppose that Handong students in campus share a 1Gbps link. Also suppose each user requires 10Mbps when transmitting, but each user transmits only 20 percent of the time. (See the discussion of packet switching versus circuit switching)**

    a. **When circuit switching is used, how many users can be supported?**

       Ans)

       $$\frac{1G}{10M} = 100 people$$

b. **For the remainder of this problem, suppose packet switching is used. Find the probability that a given user is transmitting.**

Ans)

0.2

c. **Suppose there are 150 users. Find the probability that at any given time, exactly *n* users are transmitting simultaneously. (Hint. Use the binomial distribution)**

Ans)

$$\binom{150}{n} * 0.2^n * (1 - 0.2)^{150-n}$$

d. **Find the probability that there are 31 or more users transmitting simultaneously.**

Ans)

$$1 - \sum_{n=0}^{30} \binom{150}{n} * 0.2^n * 0.8^{150-n}, \ \ m = 0.2 * 150 = 30, \sigma = \sqrt{150 * 0.2 * 0.8} = \sqrt{24}$$

$$\therefore 1 - P\left(\sum_{n=1}^{150} X_n \le 31\right), \ \ 1 - P\left(\frac{\sum_{n=1}^{150} X_n - m}{\sigma} \le \frac{31 - m}{\sigma}\right) = 1 - P\left(Z \le \frac{\sqrt{24}}{24}\right)$$

$$\approx 1 - P(Z \le 0.2041) = 1 - 0.5793 = 0.4207$$

$$\therefore 0.4207$$

3. **In this problem, we consider sending real-time voice from Host A to Host B over a packet-switched network (VoIP). Host A converts analog voice to a digital 128kbps bit stream on the fly. Host A then group the bits into 96-byte packets. There is one link between Hosts A and B; its transmission rate is 5Mbps and its propagation delay is 5msec. As soon as Host A gathers a packet, it sends it to Host B. As soon as Host B receives an entire packet, it converts the packet's bits to an analog signal. How much time elapses from the time a bit is created (from the original analog signal at Host A) until the bit is decoded (as part of the analog signal at Host B)?**
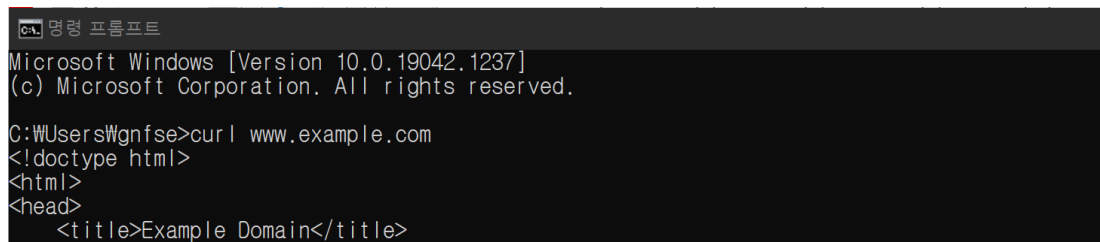
Ans)

$$\frac{96 * 8}{128 * 10^3} sec + \frac{96 * 8}{5 * 10^6} sec + 5msec = 11.15msec$$

4. **Answer the following questions after capturing the DNS and HTTP packets using *curl* and *Wireshark*. For capturing the packets, access "www.example.com" using *curl*. You have to answer with screenshots of your Wireshark.**

   Help 1: **You can find manual of Wireshark in the Internet. There are many manuals to use Wireshark!**

   Help 2: **You can use *curl* in Windows, Linux, and MacOS. Below is the *curl* executed in my desktop.**

```
명령 프롬프트
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\gnfse>curl www.example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>
```
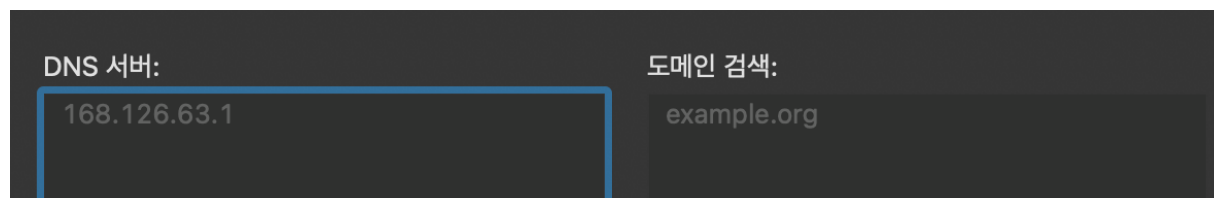
Hint 3: If you already access "www.example.com" just before you capture packets, DNS client may not send a query to DNS server since it already has cache data. In this case, you have to flush DNS. Please find the way by yourself according your OS.

   a.   What is the IP address of your default DNS server?

   Ans)

   168.126.63.1

DNS 서버:	도메인 검색:
168.126.63.1	example.org

No.	Time	Source	Destination	Protocol	Length	Info
1703	28.234482	35.74.215.78	172.17.128.169	TLSv1…	1101	Application Data
1704	28.234669	172.17.128.169	35.74.215.78	TCP	66	56747 → 443 [ACK] Seq=275 Ack=1204 Win=2031 Len=0
1705	28.411389	172.17.128.169	168.126.63.1	DNS	75	Standard query 0x32cc A www.example.com
1706	28.418189	168.126.63.1	172.17.128.169	DNS	227	Standard query response 0x32cc A www.example.com A
1707	28.419547	172.17.128.169	93.184.216.34	TCP	78	59696 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS
1708	28.422797	93.184.216.34	172.17.128.169	TCP	74	80 → 59696 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0
1709	28.422888	172.17.128.169	93.184.216.34	TCP	66	59696 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSva
1710	28.422960	172.17.128.169	93.184.216.34	HTTP	145	GET / HTTP/1.1

b. What kind of transport protocol is used for DNS packet?

Ans)

UDP 를 사용한다

```
> Frame 23591: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface en0, id 0
> Ethernet II, Src: Apple_48:31:18 (3c:a6:f6:48:31:18), Dst: RuckusWi_6d:01:ae (c0:c5:20:6d:01:ae)
> Internet Protocol Version 4, Src: 172.17.129.132, Dst: 168.126.63.1
> User Datagram Protocol, Src Port: 51211, Dst Port: 53
> Domain Name System (query)
```

c. Analyze the Flags field and query message in the DNS query packet.

Ans)

Flags: Response 가 0 이므로 Message 가 query 이다. Opcode 의 Standard query(0)은 query 의 유형이 일반 query 라는 뜻이다. Truncated 의 Message is not truncated 는 response 응답이 정해진 길이(512bytes)을 넘어서 잘렸는지 표시하는 것이다. Recursion desired 의 Do query recursively 는 query 을 보낼 때 재귀적 query 가 필요한지 나타내는데 현재는 1 로써 사용가능하다. Default 값은 1 이다 Z 의 reserved 는 나중을 위해 예약된 비트로써 0 ㅇ으로 설정한다. Non-authenticated data 는 response packet 에 사용되는데, 1 로 설정되면 response packet 이 server 에 의해 검증되었다는 뜻을 의미한다. 여기선 query packet 이므로 0 으로 설정된다.

Query message: queries 는 name-type-class 계층으로 이루어져 있는데 Name 부분에는 hostname 이 들어간다. Type 은 query 의 유형을 뜻하는데, 이 packet 에선 Host address 을 뜻하는 A 을 사용한다. 마지막으로 Class 는 네트워크 클래스 타입을 뜻하며 IN 은 Internet Class 을 뜻한다.

```
∨ Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
∨ Queries
  ∨ www.example.com: type A, class IN
      Name: www.example.com
      [Name Length: 15]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
```

d.　Analyze the answers in the DNS response packet.

Ans)

Response packet 의 flags 는 이전과 동일하지만, query packet 에서 볼 수 없었던 flag 들이 추가로 사용된다. 추가된 flag 들만 설명을 하자면, Authoritative 는 신뢰할 수 있는 DNS 의 응답인지를 표시한다. Recursion available 은 응답한 DNS server 가 recursion query 을 사용가능한지 나타내는 비트이다. 현재는 1 로써 사용 가능하다. Answer authenticated 는 answer 가 server 에 의해 authenticated 된 answer 가 반환되는지를 나타내는 것이다. Reply code 는 error 가 존재하는지 표시하며 현재는 0000 으로써 에러가 없다.

Answer RRs 는 Answer section 을 뜻한다.

Answers 은 query packet 에 대한 response 에 해당한다. 따라서 요청된 Type 에 따라 IP 주소가 포함 돼 있는 것을 볼 수 있다.

```
∨ Domain Name System (response)
     Transaction ID: 0x32cc
   ∨ Flags: 0x8180 Standard query response, No error
       1... .... .... .... = Response: Message is a response
       .000 0... .... .... = Opcode: Standard query (0)
       .... .0.. .... .... = Authoritative: Server is not an authority for domain
       .... ..0. .... .... = Truncated: Message is not truncated
       .... ...1 .... .... = Recursion desired: Do query recursively
       .... .... 1... .... = Recursion available: Server can do recursive queries
       .... .... .0.. .... = Z: reserved (0)
       .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
       .... .... ...0 .... = Non-authenticated data: Unacceptable
       .... .... .... 0000 = Reply code: No error (0)
     Questions: 1
     Answer RRs: 1
     Authority RRs: 2
     Additional RRs: 4
   ∨ Queries
     ∨ www.example.com: type A, class IN
         Name: www.example.com
         [Name Length: 15]
         [Label Count: 3]
         Type: A (Host Address) (1)
         Class: IN (0x0001)
   ∨ Answers
     ∨ www.example.com: type A, class IN, addr 93.184.216.34
         Name: www.example.com
         Type: A (Host Address) (1)
         Class: IN (0x0001)
         Time to live: 41891 (11 hours, 38 minutes, 11 seconds)
         Data length: 4
         Address: 93.184.216.34
   ∨ Authoritative nameservers
     > example.com: type NS, class IN, ns b.iana-servers.net
     > example.com: type NS, class IN, ns a.iana-servers.net
   ∨ Additional records
     > a.iana-servers.net: type A, class IN, addr 199.43.135.53
     > b.iana-servers.net: type A, class IN, addr 199.43.133.53
     > a.iana-servers.net: type AAAA, class IN, addr 2001:500:8f::53
     > b.iana-servers.net: type AAAA, class IN, addr 2001:500:8d::53
     [Request In: 1705]
     [Time: 0.006800000 seconds]
```

e.   What is the IP address of www.example.com?

Ans)

'curl www.example.com'을 했을 때, 3 handshake 와 4handshake 가 있는 것으로 보아
93.184.216.34 이다.

No.	Time	Source	Destination	Protocol	Length	Info
1703	28.234482	35.74.215.78	172.17.128.169	TLSv1…	1101	Application Data
1704	28.234669	172.17.128.169	35.74.215.78	TCP	66	56747 → 443 [ACK] Seq=
1705	28.411389	172.17.128.169	168.126.63.1	DNS	75	Standard query 0x32cc
1706	28.418189	168.126.63.1	172.17.128.169	DNS	227	Standard query respon:
1707	28.419547	172.17.128.169	93.184.216.34	TCP	78	59696 → 80 [SYN] Seq=
1708	28.422797	93.184.216.34	172.17.128.169	TCP	74	80 → 59696 [SYN, ACK]
1709	28.422888	172.17.128.169	93.184.216.34	TCP	66	59696 → 80 [ACK] Seq=
1710	28.422960	172.17.128.169	93.184.216.34	HTTP	145	GET / HTTP/1.1
1711	28.426396	93.184.216.34	172.17.128.169	TCP	66	80 → 59696 [ACK] Seq=
1712	28.744729	172.17.128.151	224.0.0.251	MDNS	152	Standard query 0x0001
1713	29.052703	93.184.216.34	172.17.128.169	TCP	1514	80 → 59696 [ACK] Seq=
1714	29.052719	93.184.216.34	172.17.128.169	HTTP	225	HTTP/1.1 200 OK (text
1715	29.052984	172.17.128.169	93.184.216.34	TCP	66	59696 → 80 [ACK] Seq=
1716	29.053509	172.17.128.169	93.184.216.34	TCP	66	59696 → 80 [FIN, ACK]
1717	29.057512	93.184.216.34	172.17.128.169	TCP	66	80 → 59696 [FIN, ACK]
1718	29.057721	172.17.128.169	93.184.216.34	TCP	66	59696 → 80 [ACK] Seq=

f.   What kind of transport protocol is used for HTTP packets?

Ans)

TCP protocol 을 사용한다.

```
> Frame 23602: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits) on interface en0, id 0
> Ethernet II, Src: RuckusWi_6d:01:ae (c0:c5:20:6d:01:ae), Dst: Apple_48:31:18 (3c:a6:f6:48:31:18)
> Internet Protocol Version 4, Src: 93.184.216.34, Dst: 172.17.129.132
> Transmission Control Protocol, Src Port: 80, Dst Port: 51635, Seq: 1449, Ack: 80, Len: 159
> [2 Reassembled TCP Segments (1607 bytes): #23601(1448), #23602(159)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (46 lines)
```

g.   What is the User-Agent field in the captured HTTP request packet? What does it mean?

Ans)

curl/7.64.1 이고 서버에게 요청할 때 쓰이는 프로그램을 뜻한다.

h.   What version of HTTP is the server running?

Ans)

HTTP 1.1 을 사용한다.

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

Ans)

200 OK

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

Ans)

Last-Modified 을 보면 Thu, 17 Oct 2019 07:18:26 GMT 인 것을 알 수 있다.

```
∨ Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Accept-Ranges: bytes\r\n
    Age: 430361\r\n
    Cache-Control: max-age=604800\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Date: Sun, 03 Oct 2021 14:37:25 GMT\r\n
    Etag: "3147526947"\r\n
    Expires: Sun, 10 Oct 2021 14:37:25 GMT\r\n
    Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT\r\n
    Server: ECS (nyb/1D0F)\r\n
    Vary: Accept-Encoding\r\n
    X-Cache: HIT\r\n
```

k.   How many bytes of content are being returned to your computer?

Ans)

1256bytes 이다.

```
  > Content-Length: 1256\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.629759000 seconds]
    [Request in frame: 1710]
    [Request URI: http://www.example.com/]
    File Data: 1256 bytes
```