컴퓨터 네트워크

Wireshark DNS, TCP Capture

20191987
이세희

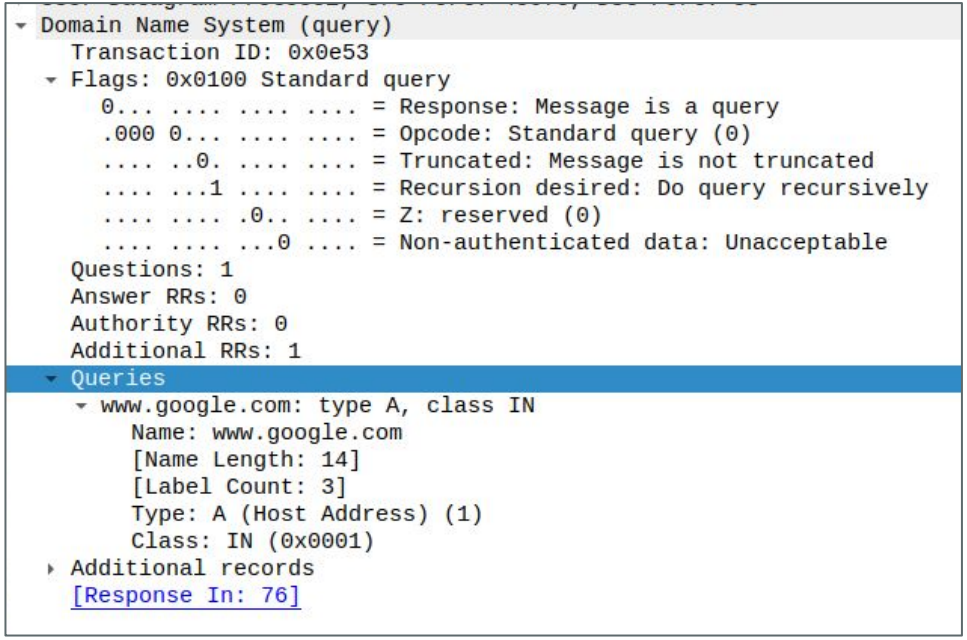
1-1. DNS query and response message: Wireshark 이용

명령어창에서 nslookup www.google.com 을 입력하여 DNS 패킷을 분석했습니다.

```
seheelee@seheelee-ThinkPad-T580:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.251.42.164
Name:   www.google.com
Address: 2404:6800:4004:821::2004
```

1-2. DNS query message: Wireshark 이용



1. **Transaction ID**
   - DNS 쿼리와 응답에 연관되는 필드이다.
   - 여기서는 0x0e53(2 byte)로 나타난다.

2. **Flags**
   a. **Response(Query)**
      - 요청하는 패킷인지 응답하는 패킷인지를 구분한다.
      - 여기서는 0에 해당하므로 요청하는 패킷을 의미한다.

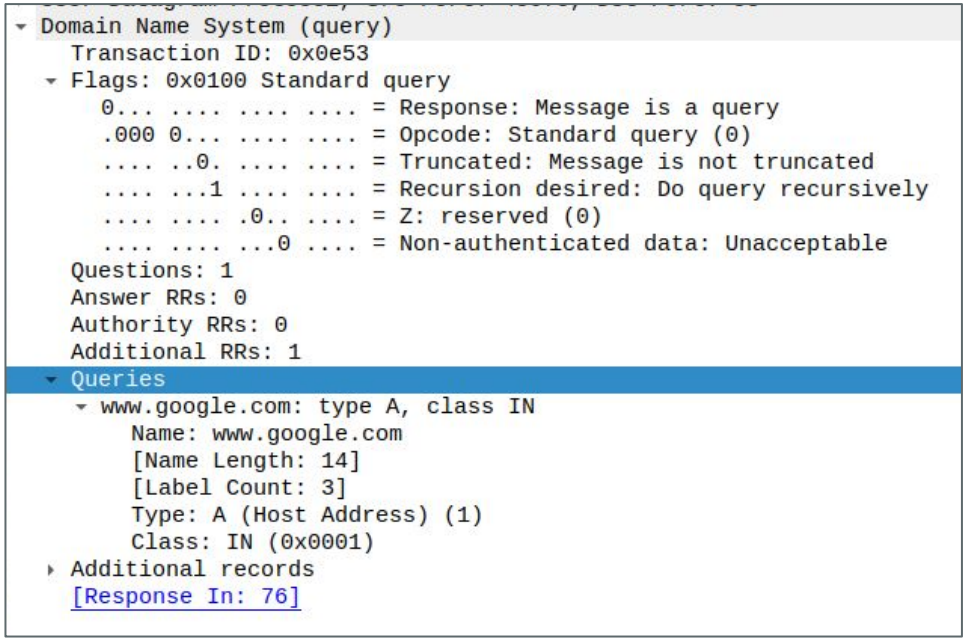
   b. **Opcode**
      - 쿼리의 유형을 지정한다.
      - 여기서는 0이 쿼리를 의미한다.

   c. **Truncation**
      - 응답이 길어서 잘렸는지에 대해 알려준다.
      - 여기서는 0으로 표시되어 잘리지 않았음을 의미한다.

   d. **Recurison Desired**
      - 재귀를 사용하는지 알려주는 비트이다.
      - 여기서는 1을 나타내어 재귀 쿼리를 사용하는 것으로 알 수 있다.

   e. **Reseved**
      - 예약된 비트이다.
      - 보통은 비워놓기 때문에 여기서도 0으로 표시되어있다.

1-2. DNS query message: Wireshark 이용



3. Question
- 질문의 개수를 표시한다.
- 여기에서는 한 개의 질문을 가지고 있다.

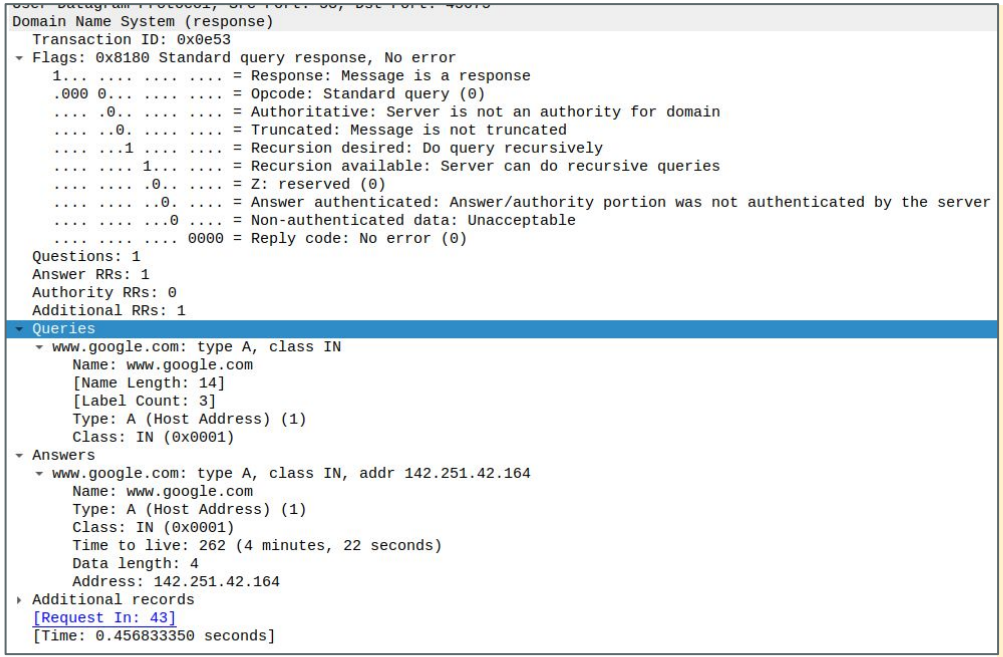
4. Answer RRs
- Answer RRs의 세션 개수를 의미한다.
- 여기서는 0개이다. 요청을 하는 것이기 때문이다.

5. Authority RRs
- Authority RRs의 세션 개수를 의미한다.
- 여기서는 0개이다.

6. Additional RRs
- Additional RRs의 세션 개수를 의미한다.
- 여기서는 0개이다.

5. Queries
- **name**
  - DNS에 요청한 도메인 네임을 의미한다.
- **Type**
  - 쿼리의 유형을 나타낸다.
  - 여기서는 호스트 주소를 의미하는 A가 나온다.
- **Class**
  - 네트워크의 클래스 타입을 표시한다.
  - IN은 internet을 의미한다.

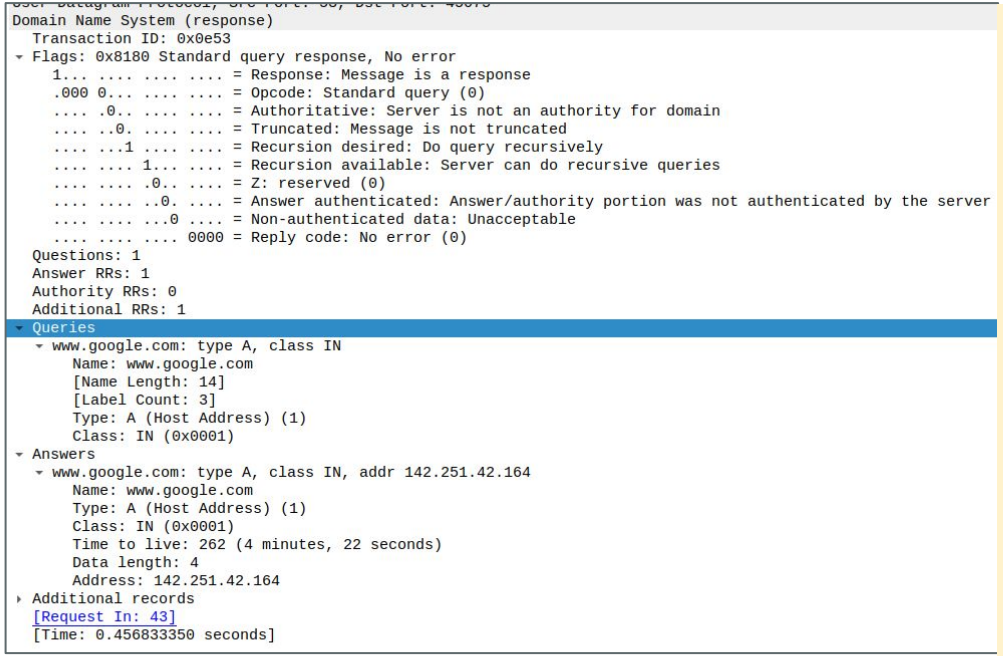
1-3. DNS response message: Wireshark 이용



1. **Transaction ID**
   - DNS 쿼리와 응답에 연관되는 필드이다.
   - 여기서는 0x0e53(2 byte)로 나타난다.

2. **Flags**
   a. **Response(Query)**
      - 요청하는 패킷인지 응답하는 패킷인지를 구분한다.
      - 여기서는 1에 해당하므로 응답하는 패킷을 의미한다.
   b. **Opcode**
      - 쿼리의 유형을 지정한다.
      - 여기서는 0이 쿼리를 의미한다.
   c. **Authoritative**
      - 공식 DNS 서버로부터의 응답인지 표시한다.
   d. **Truncation**
      - 응답이 길어서 잘렸는지에 대해 알려준다.
      - 여기서는 0으로 표시되어 잘리지 않았음을 의미한다.
   e. **Recurison desired**
      - 재귀를 사용하는지 알려주는 비트이다.
      - 여기서는 1을 나타내어 재귀 쿼리를 사용하는 것으로 알 수 있다.
   f. **Recurison available**
      - 응답에서 정의된 재귀가 사용가능한지를 표시합니다.
      - 여기에서는 1을 나타내고 있으므로 사용가능하다는 것을 알 수 있다.
   g. **Reseved**
      - 예약된 비트이다.
      - 보통은 비워놓기 때문에 여기서도 0으로 표시되어있다.

1-3. DNS response message: Wireshark 이용



2. Flags

a. Reply code

- 응답에서 오류가 존재하는지 표시하는 필드이다.
- 여기서는 0이므로 오류가 없음을 나타낸다.

3. Question

- 질문의 개수를 표시한다.
- 여기에서는 1개의 질문을 가지고 있다.

4. Answer RRs

- Answer RRs의 세션 개수를 의미한다.
- 여기서는 1개이다. 응답을 해주었기 때문이다.

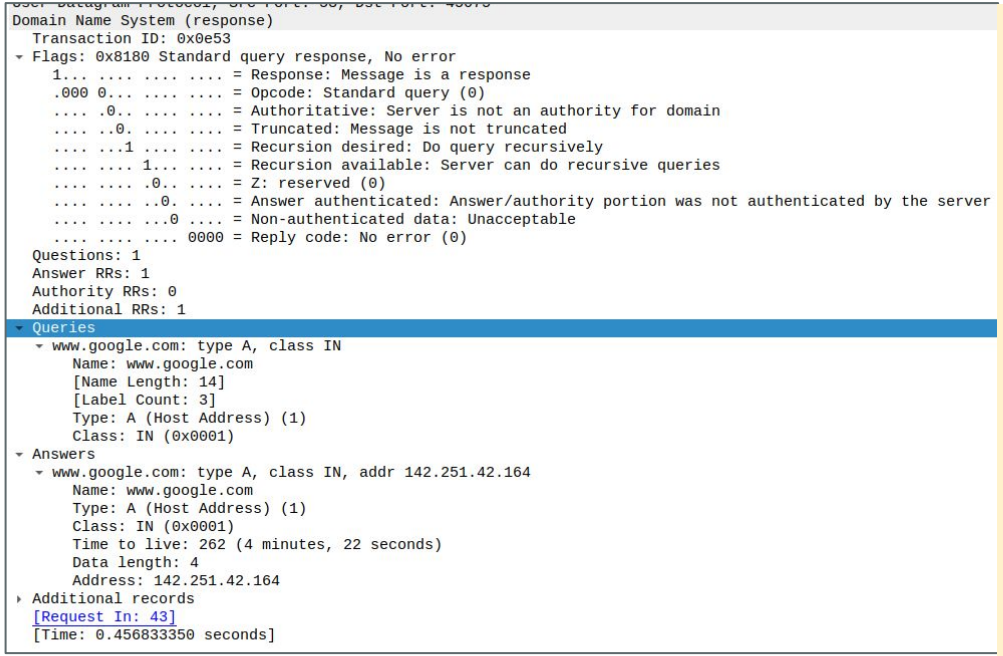
5. Authority RRs

- Authority RRs의 세션 개수를 의미한다.
- 여기서는 0개이다.

6. Additional RRs

- Additional RRs의 세션 개수를 의미한다.
- 여기서는 1개이다.

1-3. DNS response message: Wireshark 이용



5. Queries

- **name**
  - DNS에 요청한 도메인 네임을 의미한다.
- **Type**
  - 쿼리의 유형을 나타낸다.
  - 여기서는 호스트 주소를 의미하는 A가 나온다.
- **Class**
  - 네트워크의 클래스 타입을 표시한다.
  - IN은 internet을 의미한다.

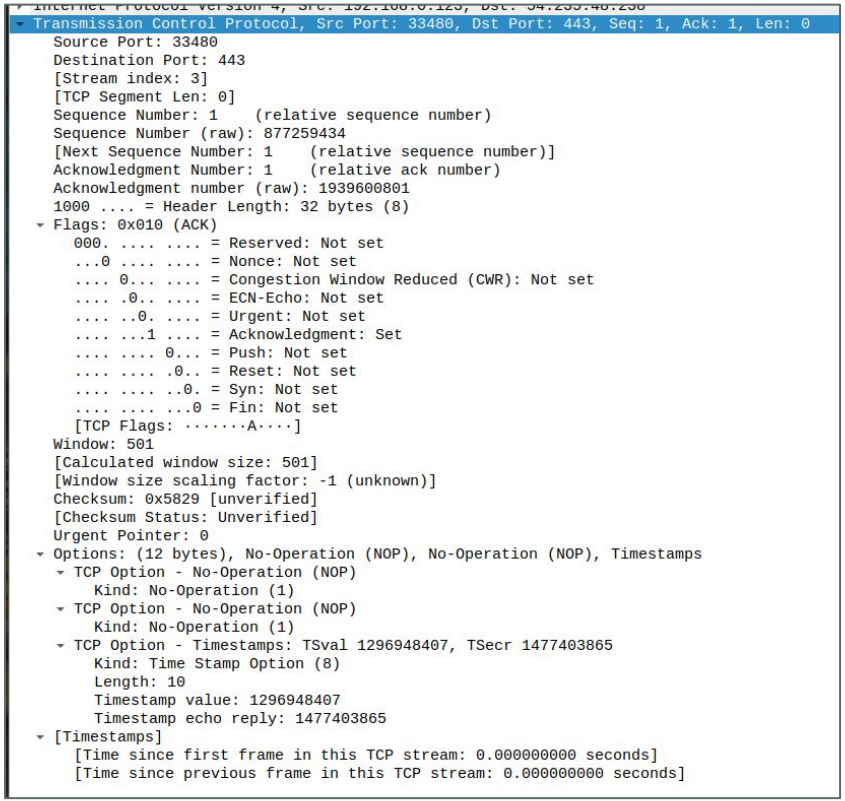
6. Answers

- **Time to live**
  - DNS 서버가 데이터를 캐싱 정보로 유지한 시간을 초로 나타낸다.
- **Data Length**
  - Rdata의 길이를 의미한다.

7. Additional records

- 다른 DNS서버에서 응답이 왔을 때 데이터가 담긴다.

2-1. TCP Segment format: Wireshark 이용



```
▸ Internet Protocol Version 4, Src: 192.168.0.123, Dst: 54.233.48.238
▾ Transmission Control Protocol, Src Port: 33480, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 33480
    Destination Port: 443
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 877259434
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1939600801
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····A····]
    Window: 501
    [Calculated window size: 501]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5829 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    ▾ TCP Option - No-Operation (NOP)
        Kind: No-Operation (1)
    ▾ TCP Option - No-Operation (NOP)
        Kind: No-Operation (1)
    ▾ TCP Option - Timestamps: TSval 1296948407, TSecr 1477403865
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 1296948407
        Timestamp echo reply: 1477403865
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.000000000 seconds]
      [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

1. **source port #**
   - 송신측의 포트번호 33480을 의미한다.

2. **dest port #**
   - 수신측의 포트번호 443을 의미한다.

3. **sequence number: counting by bytes of data(not segments) = 1**
   - TCP 세그먼트 안의 데이터의 송신 바이트 흐름의 위치를 나타낸다.

4. **acknowledgement number(not segments) = 1**
   - 수신자가 예상하는 다음 시퀀스 번호이다. 승인번호를 통해서 상대방이 데이터를 수신했다는 것을 확인할 수 있다.

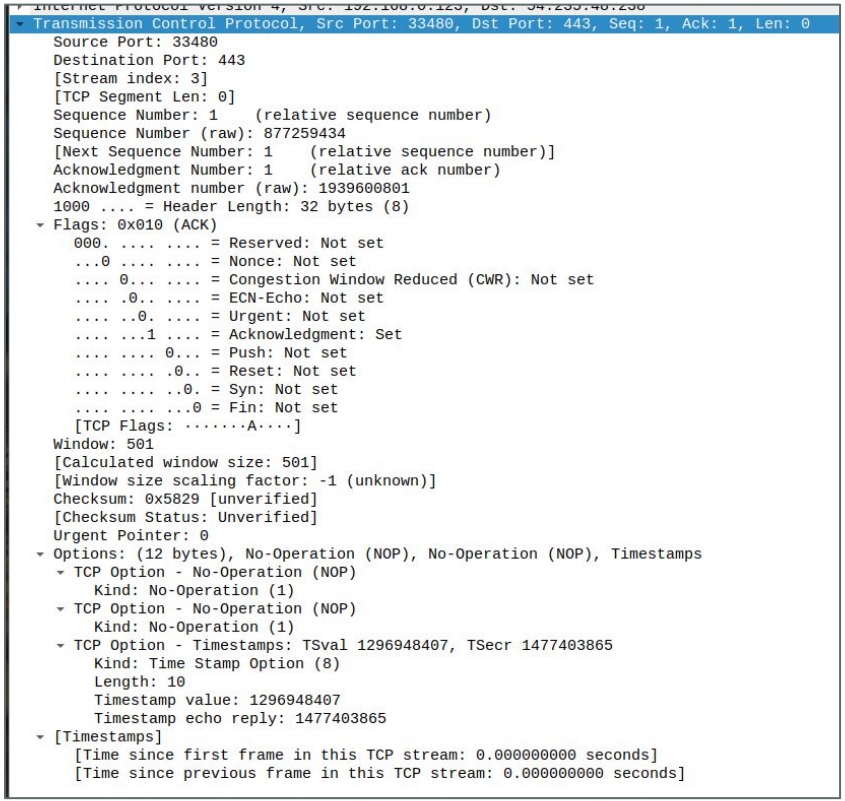
5. **header length = 8**
   - 헤더의 길이를 나타낸다.

6. **URG: urgent data pointer(generally not used) = 0(not set)**
   - Urgent pointer 필드의 값이 유효한지를 가리킨다.

7. **ACK: ACK # is valid = 1 (set)**
   - Acknowledgement 필드의 값이 유효함을 나타낸다. 클라이언트의 SYN 패킷 이후의 패킷은 모두 이 플래그가 설정 되어있어야한다.
   - 여기서는 SYN 패킷 이후 전달되는 패킷임을 알 수 있다.

8. **PSH: push data(generally not used) = 0(not set)**
   - 해당 데이터가 어플리케이션에 즉시 전달되어야할 때 수신 어플리케이션에 버퍼링된 데이터를 푸시 할건지의 여부를 나타낸다.
   - 여기서는 설정되어있지 않다.

2-1. TCP Segment format: Wireshark 이용



```
▸ Internet Protocol Version 4, Src: 192.168.0.123, Dst: 54.239.48.238
▾ Transmission Control Protocol, Src Port: 33480, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 33480
    Destination Port: 443
    [Stream index: 3]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 877259434
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1939600801
    1000 .... = Header Length: 32 bytes (8)
  ▾ Flags: 0x010 (ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
      .... .... ..0. = Syn: Not set
      .... .... ...0 = Fin: Not set
      [TCP Flags: ·····A····]
    Window: 501
    [Calculated window size: 501]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5829 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▾ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    ▾ TCP Option - No-Operation (NOP)
        Kind: No-Operation (1)
    ▾ TCP Option - No-Operation (NOP)
        Kind: No-Operation (1)
    ▾ TCP Option - Timestamps: TSval 1296948407, TSecr 1477403865
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 1296948407
        Timestamp echo reply: 1477403865
  ▾ [Timestamps]
      [Time since first frame in this TCP stream: 0.000000000 seconds]
      [Time since previous frame in this TCP stream: 0.000000000 seconds]
```

9. RST, SYN, FIN: connection management(setup, teardown commands) = 0,0,0(not set)

- RST: TCP 연결이 재설정 되어야 하는지를 의미한다.
- SYN: 양쪽이 보낸 최초의 패킷에만 설정되어있다. 연결의 시작을 알리는 의미한다.
- FIN: TCP 연결의 종료를 의미한다.
- 여기서는 세 필드 모두 유효하지 않다.

10. receive window: # bytes receiver willing to accept = 501

- 수신 윈도우의 크기를 의미한다.

11. checksum: internet checksum(as in UDP) = 0x5829

- 헤더 및 데이터의 에러 확인을 위해 사용되는 비트를 의미한다.

12. Urg data pointer = 0

- URG 플래그가 설정된 경우 시퀀스 번호로부터 오프셋을 나타낸다. 긴급 데이터의 마지막 바이트가 가지는 순서 번호이다.
- URG 플래그가 설정되어 있지 않아서 유효하지 않다.

13. options(variable length) = 12 bytes

- TCP 통신의 옵션을 나타낸다.
- 여기서는 TimeStamp 옵션이 있다.

14. application data(variable length): data sent by application into TCP socket =

- 전달하려는 데이터를 의미한다.