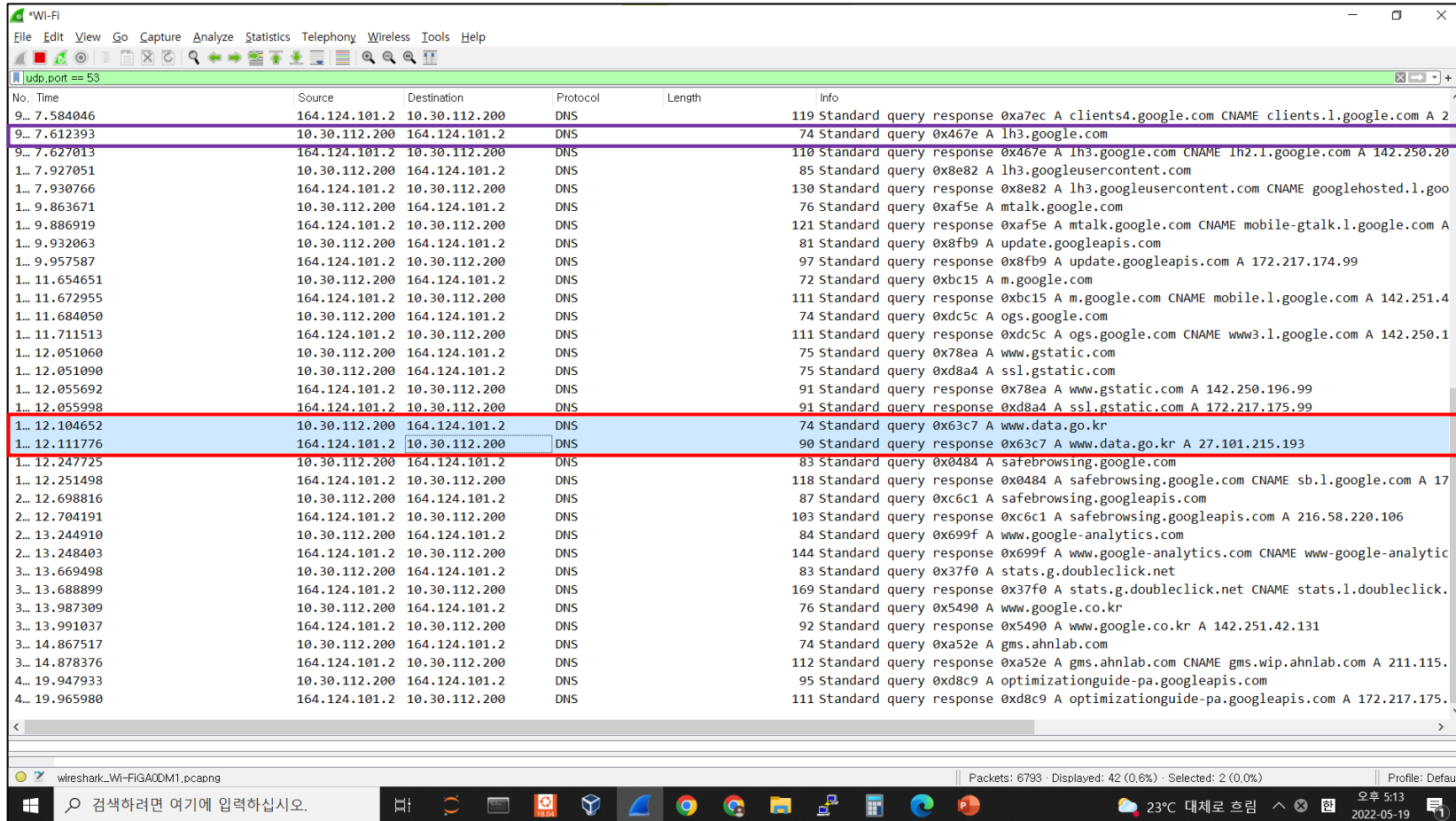


컴퓨터 네트워크(0155605-01)

# Wireshark 통신 분석

# DNS Package

## [DNS Package 전체 사진]



No.	Time	Source	Destination	Protocol	Length	Info
9...	7.584046	164.124.101.2	10.30.112.200	DNS		119 Standard query response 0xa7ec A clients4.google.com CNAME clients.l.google.com A 2
9...	7.612393	10.30.112.200	164.124.101.2	DNS		74 Standard query 0x467e A lh3.google.com
9...	7.627013	164.124.101.2	10.30.112.200	DNS		110 Standard query response 0x467e A lh3.google.com CNAME lh2.l.google.com A 142.250.20
1...	7.927051	10.30.112.200	164.124.101.2	DNS		85 Standard query 0x8e82 A lh3.googleusercontent.com
1...	7.930766	164.124.101.2	10.30.112.200	DNS		130 Standard query response 0x8e82 A lh3.googleusercontent.com CNAME googlehosted.l.goo
1...	9.863671	10.30.112.200	164.124.101.2	DNS		76 Standard query 0xaf5e A mtalk.google.com
1...	9.886919	164.124.101.2	10.30.112.200	DNS		121 Standard query response 0xaf5e A mtalk.google.com CNAME mobile-gtalk.l.google.com A
1...	9.932063	10.30.112.200	164.124.101.2	DNS		81 Standard query 0x8fb9 A update.googleapis.com
1...	9.957587	164.124.101.2	10.30.112.200	DNS		97 Standard query response 0x8fb9 A update.googleapis.com A 172.217.174.99
1...	11.654651	10.30.112.200	164.124.101.2	DNS		72 Standard query 0xbc15 A m.google.com
1...	11.672955	164.124.101.2	10.30.112.200	DNS		111 Standard query response 0xbc15 A m.google.com CNAME mobile.l.google.com A 142.251.4
1...	11.684050	10.30.112.200	164.124.101.2	DNS		74 Standard query 0xdc5c A ogs.google.com
1...	11.711513	164.124.101.2	10.30.112.200	DNS		111 Standard query response 0xdc5c A ogs.google.com CNAME www3.l.google.com A 142.250.1
1...	12.051060	10.30.112.200	164.124.101.2	DNS		75 Standard query 0x78ea A www.gstatic.com
1...	12.051090	10.30.112.200	164.124.101.2	DNS		75 Standard query 0xd8a4 A ssl.gstatic.com
1...	12.055692	164.124.101.2	10.30.112.200	DNS		91 Standard query response 0x78ea A www.gstatic.com A 142.250.196.99
1...	12.055998	164.124.101.2	10.30.112.200	DNS		91 Standard query response 0xd8a4 A ssl.gstatic.com A 172.217.175.99
1...	12.104652	10.30.112.200	164.124.101.2	DNS		74 Standard query 0x63c7 A www.data.go.kr
1...	12.111776	164.124.101.2	10.30.112.200	DNS		90 Standard query response 0x63c7 A www.data.go.kr A 27.101.215.193
1...	12.247725	10.30.112.200	164.124.101.2	DNS		83 Standard query 0x0484 A safebrowsing.google.com
1...	12.251498	164.124.101.2	10.30.112.200	DNS		118 Standard query response 0x0484 A safebrowsing.google.com CNAME sb.l.google.com A 17
2...	12.698816	10.30.112.200	164.124.101.2	DNS		87 Standard query 0xc6c1 A safebrowsing.googleapis.com
2...	12.704191	164.124.101.2	10.30.112.200	DNS		103 Standard query response 0xc6c1 A safebrowsing.googleapis.com A 216.58.220.106
2...	13.244910	10.30.112.200	164.124.101.2	DNS		84 Standard query 0x699f A www.google-analytics.com
2...	13.248403	164.124.101.2	10.30.112.200	DNS		144 Standard query response 0x699f A www.google-analytics.com CNAME www-google-analytic
3...	13.669498	10.30.112.200	164.124.101.2	DNS		83 Standard query 0x37f0 A stats.g.doubleclick.net
3...	13.688899	164.124.101.2	10.30.112.200	DNS		169 Standard query response 0x37f0 A stats.g.doubleclick.net CNAME stats.l.doubleclick.
3...	13.987309	10.30.112.200	164.124.101.2	DNS		76 Standard query 0x5490 A www.google.co.kr
3...	13.991037	164.124.101.2	10.30.112.200	DNS		92 Standard query response 0x5490 A www.google.co.kr A 142.251.42.131
3...	14.867517	10.30.112.200	164.124.101.2	DNS		74 Standard query 0xa52e A gms.ahnlab.com
3...	14.878376	164.124.101.2	10.30.112.200	DNS		112 Standard query response 0xa52e A gms.ahnlab.com CNAME gms.wip.ahnlab.com A 211.115.
4...	19.947933	10.30.112.200	164.124.101.2	DNS		95 Standard query 0xd8c9 A optimizationguide-pa.googleapis.com
4...	19.965980	164.124.101.2	10.30.112.200	DNS		111 Standard query response 0xd8c9 A optimizationguide-pa.googleapis.com A 172.217.175.

## [전체 상황]

- UDA PORT 53 진행
  - 구글(google) 접속 후 공공 데이터 포털 ([www.data.go.kr](http://www.data.go.kr)) 접속 진행
  - 왼쪽 사진이 진행한 DNS Package 결과
- ① 보란색 박스(준비 단계): Google 접속
  - ② 빨간색 박스(실행 단계): 접속 **DNS Package 결과**

# DNS Query (Response)

No.	Time	Source	Destination	Protocol	Length	Info
12.055692		164.124.101.2	10.30.112.200	DNS		91 Standard query response 0x78ea A www.gstatic.com A 142.250.196.99
12.055998		164.124.101.2	10.30.112.200	DNS		91 Standard query response 0xd8a4 A ssl.gstatic.com A 172.217.175.99
12.104652		10.30.112.200	164.124.101.2	DNS		74 Standard query 0x63c7 A www.data.go.kr
12.111776		164.124.101.2	10.30.112.200	DNS		90 Standard query response 0x63c7 A www.data.go.kr A 27.101.215.193
12.247725		10.30.112.200	164.124.101.2	DNS		83 Standard query 0x0484 A safebrowsing.google.com
12.251498		164.124.101.2	10.30.112.200	DNS		118 Standard query response 0x0484 A safebrowsing.google.com CNAME sb.l.google.com A 17

## Query Message

```
> Frame 1815: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
> Ethernet II, Src: IntelCor_a1:ec:67 (84:1b:77:a1:ec:67), Dst: IETF-VRRP-VR
> Internet Protocol Version 4, Src: 10.30.112.200, Dst: 164.124.101.2
> User Datagram Protocol, Src Port: 57402, Dst Port: 53
  Domain Name System (query)
    Transaction ID: 0x63c7
    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.data.go.kr: type A, class IN
        [Response In: 1822]
```

```
0000  00 00 5e 00 01 70 84 1b 77 a1 ec 67 08 00 45 00  ..^..p.. w..g..E.
0010  00 3c ec c5 00 00 80 11 00 00 0a 1e 70 c8 a4 7c  <..... ..p..|
0020  65 02 e0 3a 00 35 00 28 84 9e 63 c7 01 00 00 01  e...5.(..c.....
0030  00 00 00 00 00 00 03 77 77 77 04 64 61 74 61 02  ....w ww.data.
0040  67 6f 02 6b 72 00 00 01 00 01  go.kr... ..
```

Domain Name System (dns), 32 byte(s)

IPv4 사용하여 **Client(10.30.112.200) => DNS(164.124.101.2)**

Query response

- **UDP** 사용함(Client의 un-known port 사용)
- Client(source) port: 57402 / DNS(Destination) port: 53 사용 확인
- Transaction ID(DNS 관한 정보를 보기 위한 Filtering ID): 63C7
- **식별 값**으로 응답에 대한 특정 질의라는 사실을 알려줌

# DNS Query (Response)

## [1] Flags

구성 요소	값	의미(분석)
Response	0	요청하는 패킷을 의미(Query Package)
Opcode	0000	표준 쿼리를 의미(메시지 생성한 쿼리 종류)
Truncated	0	응답이 길어져서 잘린 비트가 없음을 의미
Recursion Desired	1	Client가 요청하는 순환 Query문 의미(재귀 쿼리)
Z	0	예약된 비트 의미

## [2] Flags 아래 부분

구성 요소	값	의미(분석)
Questions	1	패킷이 하나의 질문을 가짐
Answer RRs	0	응답 session(질의 packing)의 개수가 0
Authority RRs	0	신뢰 Session의 네임 서버의 RR 개수가 0
Additional RRs	0	추가적인 엔트리의 개수가 0

> Frame 1815: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i  
> Ethernet II, Src: IntelCor\_a1:ec:67 (84:1b:77:a1:ec:67), Dst: IETF-VRRP-VR  
> Internet Protocol Version 4, Src: 10.30.112.200, Dst: 164.124.101.2  
> User Datagram Protocol, Src Port: 57402, Dst Port: 53  
▼ Domain Name System (query)  
Transaction ID: 0x63c7  
▼ 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.data.go.kr: type A, class IN  
[\[Response In: 1822\]](#)

0000 00 00 5e 00 01 70 84 1b 77 a1 ec 67 08 00 45 00 ..^..p.. w..g..E  
0010 00 3c ec c5 00 00 80 11 00 00 0a 1e 70 c8 a4 7c <.....p..|  
0020 65 02 e0 3a 00 35 00 28 84 9e 63 c7 01 00 00 01 e...:5.( ..c.....  
0030 00 00 00 00 00 00 03 77 77 77 04 64 61 74 61 02 .....w ww.data.  
0040 67 6f 02 6b 72 00 00 01 00 01 go.kr... ..

Domain Name System (dns), 32 byte(s)

- 최초로 Response 진행해서 Question 요소(요청)에 대한 정보만 가짐
- 아직 응답을 받지 않았기에 Answer RRs = 0, Authority RRs = 0(응답자체가 없음)
- 추가적인 session 역시 동일한 앞선 이유와 동일 /

# DNS Query (Response)

```

> Frame 1815: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on i
> Ethernet II, Src: IntelCor_a1:ec:67 (84:1b:77:a1:ec:67), Dst: IETF-VRRP-VR
> Internet Protocol Version 4, Src: 10.30.112.200, Dst: 164.124.101.2
> User Datagram Protocol, Src Port: 57402, Dst Port: 53
  < Domain Name System (query)
    Transaction ID: 0x63c7
    < 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.data.go.kr: type A, class IN
      [Response In: 1822]
  
```

0000	00 00 5e 00 01 70 84 1b 77 a1 ec 67 08 00 45 00	..^..p.. w..g..E..
0010	00 3c ec c5 00 00 80 11 00 00 0a 1e 70 c8 a4 7c	<.....p..
0020	65 02 e0 3a 00 35 00 28 84 9e 63 c7 01 00 00 01	e...:5.( ..c.....
0030	00 00 00 00 00 00 03 77 77 77 04 64 61 74 61 02	.....w ww.data..
0040	67 6f 02 6b 72 00 00 01 00 01	go.kr... ..

Domain Name System (dns), 32 byte(s)

```

  < Queries
    < www.data.go.kr: type A, class IN
      Name: www.data.go.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      [Response In: 1822]
  
```

Query 내용을 구체적으로 보여줌

구성 요소	값	의미(분석)
Name	1	<b>DNS에 요청하는 Domain Name</b> 이 "www.data.go.kr"
Type	0	Query의 유형이 Text
Class	0	Network 유형이 Inter-Net(IN)



- (파란색 Drag 부분): Query Head 부분
- (빨간색 바 이전) : Flag 부분 정보
- (빨간색 바 이후) : Query 부분 정보

# DNS Query (Request)

No.	Time	Source	Destination	Protocol	Length	Info
12.055692		164.124.101.2	10.30.112.200	DNS		91 Standard query response 0x78ea A www.gstatic.com A 142.250.196.99
12.055998		164.124.101.2	10.30.112.200	DNS		91 Standard query response 0xd8a4 A ssl.gstatic.com A 172.217.175.99
12.111776		164.124.101.2	10.30.112.200	DNS		90 Standard query response 0x63c7 A www.data.go.kr A 27.101.215.193
12.247725		10.30.112.200	164.124.101.2	DNS		85 Standard query 0x0484 A safebrowsing.google.com
12.251498		164.124.101.2	10.30.112.200	DNS		118 Standard query response 0x0484 A safebrowsing.google.com CNAME sb.l.google.com A 17

```

> Frame 1822: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF{...}
> Ethernet II, Src: Dell_a7:e8:a0 (d8:9e:f3:a7:e8:a0), Dst: IntelCor_a1:ec:67 (84:1b:77:a1:ec:67)
> Internet Protocol Version 4, Src: 164.124.101.2, Dst: 10.30.112.200
> User Datagram Protocol, Src Port: 53, Dst Port: 57402
< Domain Name System (response)
  Transaction ID: 0x63c7
  Flags: 0x8180 Standard query response, No error
    1... .. = Response: Message is a response
    0000... .. = Opcode: Standard query (0)
    ... .. = Authoritative: Server is not an authority for domain
    ... .. = Truncated: Message is not truncated
    ... .. = Recursion desired: Do query recursively
    ... .. = Recursion available: Server can do recursive queries
    ... .. = Z: reserved (0)
    ... .. = Answer authenticated: Answer/authority portion was not authenticated
    ... .. = Non-authenticated data: Unacceptable
    ... .. = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.data.go.kr: type A, class IN
      Name: www.data.go.kr
      [Name Length: 14]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Answers
    www.data.go.kr: type A, class IN, addr 27.101.215.193
      Name: www.data.go.kr
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 262 (4 minutes, 22 seconds)
      Data length: 4
      Address: 27.101.215.193
  [Request In: 1815]
0000 84 1b 77 a1 ec 67 d8 9e f3 a7 e8 a0 08 00 45 00
0010 00 4c 3a 7f 40 00 37 11 84 bd a4 7c 65 02 0a 1e
0020 70 c8 00 35 e0 3a 00 38 e3 79 63 c7 81 80 00 01
0030 00 01 00 00 00 00 03 77 77 77 04 64 61 74 61 02
0040 67 6f 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01
0050 00 00 01 06 00 04 1b 65 d7 c1

```

- IPv4 사용하여 DNS(164.124.101.2) => Client(10.30.112.200)  
Request response
- UDP 사용함(Client의 un-known port 사용)
- DNS(source) port: 53 / Client(Destination) port: 57402 사용 확인  
=> **Query Packet과 통신이 source, Destination 반대로 진행**
- Transaction ID(DNS 관한 정보를 보기 위한 Filtering ID): 63C7  
=> (당연히) **Require와 동일한 Transaction ID를 지님**

# DNS Query (Request)

Domain Name System (response)  
Transaction ID: 0x63c7

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
- .... 0... .. = Non-authenticated data: Unacceptable
- .... 0000 = Reply code: No error (0)

Questions: 1  
Answer RRs: 1  
Authority RRs: 0  
Additional RRs: 0

Queries

- www.data.go.kr: type A, class IN
  - Name: www.data.go.kr
  - [Name Length: 14]
  - [Label Count: 4]
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)

Answers

- www.data.go.kr: type A, class IN, addr 27.101.215.193
  - Name: www.data.go.kr
  - Type: A (Host Address) (1)
  - Class: IN (0x0001)
  - Time to live: 262 (4 minutes, 22 seconds)
  - Data length: 4
  - Address: 27.101.215.193

[Request In: 1815]

```

0000 84 1b 77 a1 ec 67 d8 9e f3 a7 e8 a0 08 00 45 00
0010 00 4c 3a 7f 40 00 37 11 84 bd a4 7c 65 02 0a 1e
0020 70 c8 00 35 e0 3a 00 38 e3 79 63 c7 81 80 00 01
0030 00 01 00 00 00 00 03 77 77 77 04 64 61 74 61 02
0040 67 6f 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01
0050 00 00 01 06 00 04 1b 65 d7 c1
  
```

(추가/변경) 구성 요소	값	의미(분석)
Response	1	응답하는 패킷을 의미(Response Package)
Authoritative	0	공식 DNS 서버로부터 온 응답은 아님
Recurision Available	1	응답에서 재귀가 사용 가능함
Reply Code	0000	응답에 오류가 없었음 참고자료(0: 오류 없음 / 1: 형식 오류 / 2: 서버 실패 / 3. 존재하지 않는 이름 / 4. 실행 안됨 / 5. 거부)

구성 요소	값	의미(분석)
Questions	1	패킷이 하나의 질문을 가짐(Query)
Answer RRs	1	응답 session(질의 packing)의 개수가 1
Authority RRs	0	신뢰 Session의 네임 서버의 RR 개수가 0
Additional RRs	0	추가적인 엔트리의 개수가 0

- 요청 패킷에 Question 개수만 1였지만, **응답 패킷 (응답해) Answer RRs 개수가 1임**
- **공식 DNS 서버에서 응답을 주지 않았기에 0으로 제공**



# DNS Query (Request)

Domain Name System (response)
Transaction ID: 0x63c7
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 authen
....0... .. = Non-authenticated data: Unacceptable
....0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0

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

Answers
www.data.go.kr: type A, class IN, addr 27.101.215.193
Name: www.data.go.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 262 (4 minutes, 22 seconds)
Data length: 4
Address: 27.101.215.193
[Request In: 1815]

0000 84 1b 77 a1 ec 67 d8 9e f3 a7 e8 a0 08 00 45 00
0010 00 4c 3a 7f 40 00 37 11 84 bd a4 7c 65 02 0a 1e
0020 70 c8 00 35 e0 3a 00 38 e3 79 63 c7 81 80 00 01
0030 00 01 00 00 00 00 03 77 77 77 04 64 61 74 61 02
0040 67 6f 02 6b 72 00 00 01 00 01 c0 0c 00 01 00 01
0050 00 00 01 06 00 04 1b 65 d7 c1

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

Answers
www.data.go.kr: type A, class IN, addr 27.101.215.193
Name: www.data.go.kr
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 262 (4 minutes, 22 seconds)
Data length: 4
Address: 27.101.215.193
[Request In: 1815]
[Time: 0.007124000 seconds]

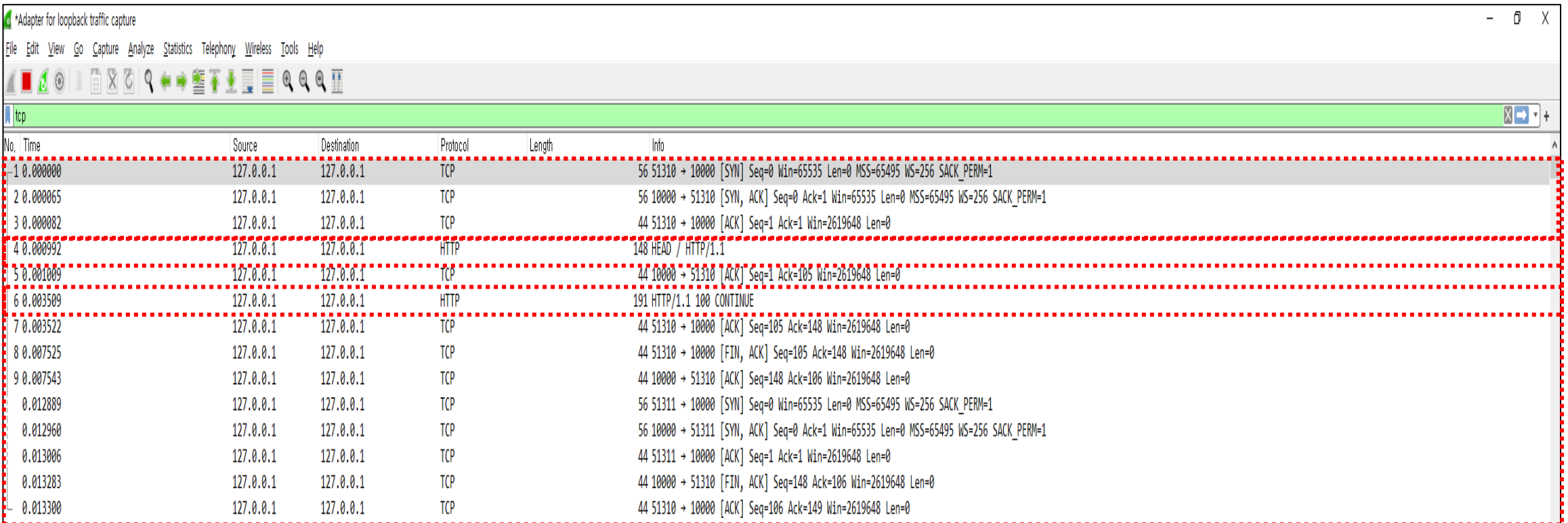
Query의 내용은 **이전 Query Packing은 동일**(해당 Query를 바탕으로 Response)

구성 요소	값	의미(분석)
Time to live	262	DNS 서버가 <b>데이터를 Cashing</b> 으로 유지한 시간이 4분 22초
Data Length	4	Rdata(해당 <b>Resource</b> 담고 있는 실제 정보) 길이
Address	27.101.215.193	<a href="http://www.data.co.kr">www.data.co.kr</a> 해당하는 IP주소

- (파란색 Drag 부분): Query Head 부분
- (첫번째 빨간색 바 이전) : Flag 부분 정보
- (첫번째 ~ 두번째 바 사이) : Query 부분 정보
- (두번째 바 이후) : Answer 부분 정보



# TCP Segment



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	51310 → 10000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
2	0.000065	127.0.0.1	127.0.0.1	TCP	56	10000 → 51310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
3	0.000082	127.0.0.1	127.0.0.1	TCP	44	51310 → 10000 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
4	0.000992	127.0.0.1	127.0.0.1	HTTP	148	HEAD / HTTP/1.1
5	0.001009	127.0.0.1	127.0.0.1	TCP	44	10000 → 51310 [ACK] Seq=1 Ack=105 Win=2619648 Len=0
6	0.003509	127.0.0.1	127.0.0.1	HTTP	191	HTTP/1.1 100 CONTINUE
7	0.003522	127.0.0.1	127.0.0.1	TCP	44	51310 → 10000 [ACK] Seq=105 Ack=148 Win=2619648 Len=0
8	0.007525	127.0.0.1	127.0.0.1	TCP	44	51310 → 10000 [FIN, ACK] Seq=105 Ack=148 Win=2619648 Len=0
9	0.007543	127.0.0.1	127.0.0.1	TCP	44	10000 → 51310 [ACK] Seq=148 Ack=106 Win=2619648 Len=0
10	0.012889	127.0.0.1	127.0.0.1	TCP	56	51311 → 10000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
11	0.012960	127.0.0.1	127.0.0.1	TCP	56	10000 → 51311 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
12	0.013006	127.0.0.1	127.0.0.1	TCP	44	51311 → 10000 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
13	0.013283	127.0.0.1	127.0.0.1	TCP	44	10000 → 51310 [FIN, ACK] Seq=148 Ack=106 Win=2619648 Len=0
14	0.013300	127.0.0.1	127.0.0.1	TCP	44	51310 → 10000 [ACK] Seq=106 Ack=149 Win=2619648 Len=0

- 중간고사 과제로 진행했던 HTTP 통신을 통해서 TCP 내용 분석 진행 (Local 내에서 통신 진행)

- ① **Local 컴퓨터**(source, 127.0.0.1 / Destination, 127.0.0.1) 내에서 **3-way Handshaking** 통해 연결
- ② 연결 후 Client가 **서버에게 HTTP 요청함**
- ③ 서버가 Client가 **HTTP로 응답함**
- ④ 파일을 전송한 이후 **연결을 해제**

# TCP Segment

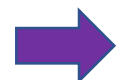
## [1] TCP(HTTP 통신 간) 해석

4 0.000992	127.0.0.1	127.0.0.1	HTTP	148 HEAD / HTTP/1.1
5 0.001009	127.0.0.1	127.0.0.1	TCP	44 10000 → 51310 [ACK] Seq=1 Ack=105 Win=2619648 Len=0
6 0.003509	127.0.0.1	127.0.0.1	HTTP	191 HTTP/1.1 100 CONTINUE

```

> Frame 5: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 10000, Dst Port: 51310, Seq: 1, Ack: 105, Len: 0
  Source Port: 10000
  Destination Port: 51310
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3362868226
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 105 (relative ack number)
  Acknowledgment number (raw): 3123076333
  0101 ... = Header Length: 20 bytes (5)
  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: 10233
  [Calculated window size: 2619648]
  [Window size scaling factor: 256]
  Checksum: 0x6ed2 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
    [Time since first frame in this TCP stream: 0.001009000 seconds]
    [Time since previous frame in this TCP stream: 0.000017000 seconds]
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 4]
    [The RTT to ACK the segment was: 0.000017000 seconds]
    [iRTT: 0.000082000 seconds]
0000 02 00 00 00 45 00 00 28 42 bc 40 00 80 06 00 00
0010 7f 00 00 01 7f 00 00 01 27 10 c8 6e c8 71 4c 02
0020 ba 26 5c ed 50 10 27 f9 6e d2 00 00

```



Source Port: 10000			Destination Port:53310		
Sequence(순서번호): 1					
ACK(응답번호): 105					
HL: 20 byte		예약(0)	Flag: syn 0		Window size: 10233
TCP Check-Sum(체크섬): 0x6ed2(False)				Urgent point: 0	

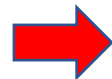


- Source Port(출발지) 51310 => Destination Port(목적지) 10000 연결 시도
- Sequence Number(순서번호): 1로 **Hand-shaking** 이후 현재 session 내에서 누적 Sequence 번호로 1
- ACK(응답번호): 105로 Client 받은 HTTP Packing의 Segment 크기가 104byte로 104 + sequence Number로 105 값이 할당(수신자가 예상하는 Sequence 번호)
- 순서 번호(Sequence, ACK)의 경우 쉽게 보기 위해 상대적인 값으로 1, 105 표현되고, 실제 Raw 값은 해당 번호 아래의 기입됨(ex: Sequence => 3362868226 )
- TCP Header의 크기는 필드 값이 4bytes 증가해 20byte를 가짐

# TCP Segment

## [1] TCP(HTTP 통신 간) 해석

```
> Frame 5: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_{...}
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 10000, Dst Port: 51310, Seq: 1, Ack: 105, Len: 0
  Source Port: 10000
  Destination Port: 51310
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 3362868226
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 105 (relative ack number)
  Acknowledgment number (raw): 3123076333
  0101 ..... Header Length: 20 bytes (5)
  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: 10233
  [Calculated window size: 2619648]
  [Window size scaling factor: 256]
  Checksum: 0x6ed2 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
    [Time since first frame in this TCP stream: 0.001009000 seconds]
    [Time since previous frame in this TCP stream: 0.000017000 seconds]
  [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 4]
    [The RTT to ACK the segment was: 0.000017000 seconds]
    [RTT: 0.000082000 seconds]
0000 02 00 00 00 45 00 00 28 42 bc 40 00 80 06 00 00
0010 7f 00 00 01 7f 00 00 01 27 10 c8 6e c8 71 4c 02
0020 ba 26 5c ed 50 10 27 f9 6e d2 00 00
```



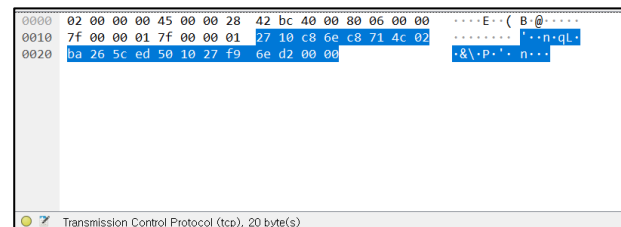
구성 요소	값	의미(분석)
Reserved	0	예약된 필드로 0으로 채움
Nonce	0	- Network 상에서 <b>혼잡하지 않아서</b> , 전송 속도 조절 x - Explicit Congestion Notification 관련된 구성 요소
CWR	0	- Host가 <b>TCP segment</b> 수신 CWM에 의해 응답(not set) - (0 : 송신자의 <b>window size</b> 를 줄이지 않음)
ECN-Echo	0	- 정상적인 전송 중에 수신이 됨( <b>혼잡하지 않음</b> ) - Congestion 상황 시 수신자 => 송신자 알리는 역할
Urgent	0	<b>긴급하게 처리해야 하는 데이터가 없음</b>
acknowledgment	1	SYN에 대한 <b>확인 응답</b> 이 되었음(set)
Push	0	데이터를 응용 계층으로 보내지 말라(not set)
Reset	0	<b>TCP 연결을 재전송할 필요 없음(not set)</b> (송신자의 유효 연결 시도 + 통신 연결 과정 정상적으로 작동하고 있음을 의미)
Syn	0	- 호스트 간의 <b>순서번호를 동기화</b> 할 필요 없음(not set) - 해당 단계는 TCP hand shaking 단계에서 진행 (통신 시작 시 연결을 요청 및 응답을 교환하는 역할)
Fin	0	- <b>데이터 전송을 종료</b> 하지 않음(프로세스 완료 / not set) - <b>Calculated window size: 2619648</b> 가 있어서 종료하지 않음(0일 경우, 중단[FIN, ACK] 사인을 보냄)

# TCP Segment

## [1] TCP(HTTP 통신 간) 해석

```
> Frame 5: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface \Device\NPF_{...}
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
✓ Transmission Control Protocol, Src Port: 10000, Dst Port: 51310, Seq: 1, Ack: 105, Len: 0
  Source Port: 10000
  Destination Port: 51310
  [Stream index: 0]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 336288226
  [Next Sequence Number: 1 (relative sequence number)]
  Acknowledgment Number: 105 (relative ack number)
  Acknowledgment number (raw): 3123076333
  0101 .... = Header Length: 20 bytes (5)
  ✓ 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: 10233
  [Calculated window size: 2619648]
  [Window size scaling factor: 256]
  Checksum: 0x6ed2 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
    [Time since first frame in this TCP stream: 0.001009000 seconds]
    [Time since previous frame in this TCP stream: 0.000017000 seconds]
  ✓ [SEQ/ACK analysis]
    [This is an ACK to the segment in frame: 4]
    [The RTT to ACK the segment was: 0.000017000 seconds]
    [RTT: 0.000002000 seconds]
  0000 02 00 00 00 45 00 00 28 42 bc 40 00 80 06 00 00
  0010 7f 00 00 01 7f 00 00 01 27 10 c8 6e c8 71 4c 02
  0020 ba 26 5c ed 50 10 27 f9 6e d2 00 00
```

구성 요소	값	의미(분석)
Window	10233	TCP 수신 <b>Buffer</b> 의 크기가 10,233byte
Check-sum Field	unverified	<b>Header 및 data의 error가 없음</b> (unverified)
Urgent Pointer	0	<b>마지막 긴급 데이터가 없음으로 =&gt; 긴급 데이터 바이 당연히 0</b>



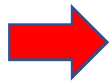
Format 내용	실제 값	아래 표현(header)	대응 표현
Source port	10000	27 10	' .
Destination port	51310	C8 6e	• n
Sequence number	336288226(상대 값:1)	C8 71 4c 02	• qL •
ACK number	3123076333(상대 값: 105)	Ba 26 5c ed	• &W •
Flags	0x010	50 10	P •
Window size	10233	27 f9	27 f9
Checksum	0x6ed2(unverified)	6e d1	n •
Urgent pointer	0	00 00	• •

# TCP Segment

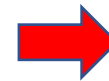
## [2] Hand Shaking 과정 / Option 정보 추가해 분석 진행

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	51310 → 10000 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
2	0.000065	127.0.0.1	127.0.0.1	TCP	56	10000 → 51310 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
3	0.000082	127.0.0.1	127.0.0.1	TCP	44	51310 → 10000 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

Transmission Control Protocol, Src Port: 51310, Dst Port: 10000, Seq: 0, Len: 0  
Source Port: 51310  
Destination Port: 10000  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 3123076228  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 0  
Acknowledgment number (raw): 0  
1000 .... = Header Length: 32 bytes (8)  
▼ Flags: 0x002 (SYN)  
000. .... = Reserved: Not set  
...0 .... = Nonce: Not set  
... 0... = Congestion Window Reduced (CWR): Not set  
... .0.. = ECN-Echo: Not set  
... ..0. = Urgent: Not set  
... ...0 = Acknowledgment: Not set  
... ....0... = Push: Not set  
... .....0.. = Reset: Not set  
> .... ..1. = Syn: Set  
... ..0 = Fin: Not set  
[TCP Flags: .....S.]



Transmission Control Protocol, Src Port: 10000, Dst Port: 51310, Seq: 0, Ack: 1, Len: 0  
Source Port: 10000  
Destination Port: 51310  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 3362868225  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 3123076229  
1000 .... = Header Length: 32 bytes (8)  
▼ Flags: 0x012 (SYN, 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  
... ...0 = Acknowledgment: Set  
... ....0... = Push: Not set  
... .....0.. = Reset: Not set  
> .... ..1. = Syn: Set  
... ..0 = Fin: Not set  
[TCP Flags: .....A..S.]



Transmission Control Protocol, Src Port: 51310, Dst Port: 10000, Seq: 1, Ack: 1, Len: 0  
Source Port: 51310  
Destination Port: 10000  
[Stream index: 0]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 3123076229  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 3362868226  
0101 .... = Header Length: 20 bytes (5)  
▼ 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  
... ...0 = Acknowledgment: Set  
... ....0... = Push: Not set  
... .....0.. = Reset: Not set  
... ..0. = Syn: Not set  
... ..0 = Fin: Not set  
[TCP Flags: .....A....]

- Client가 통신하기 위해 Server에 전송

[1] 임의의 포트 번호(51310)

[2] SYNbit =1

[3] Sequence number 0으로 할당(최초)

- Server에서 SYN 요청 받고 난 뒤 received message

[1] SYNbit =1 (유지)

[2] 응답으로 ACK =1(sequence[0] + 1)

[3] SYN + ACK 정보 전달(Client의 connection 열린 상황)

- Client가 서버의 SYN + ACK에 대한 SCK  
(message 받았다고 알리는 상황)

- Sequence number: 1, ACK number = 1)

- Server의 connection 열림

# TCP Segment

## [2] Hand Shaking 과정 / Option 정보 추가해 분석 진행

Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted  
 ✓ TCP Option - Maximum segment size: 65495 bytes  
     Kind: Maximum Segment Size (2)  
     Length: 4  
     MSS Value: 65495  
 ✓ TCP Option - No-Operation (NOP)  
     Kind: No-Operation (1)  
 ✓ TCP Option - Window scale: 8 (multiply by 256)  
     Kind: Window Scale (3)  
     Length: 3  
     Shift count: 8  
     [Multiplier: 256]  
 ✓ TCP Option - No-Operation (NOP)  
     Kind: No-Operation (1)  
 ✓ TCP Option - No-Operation (NOP)  
     Kind: No-Operation (1)  
 ✓ TCP Option - SACK permitted  
     Kind: SACK Permitted (4)  
     Length: 2

- Hand Shaking 과정 중 첫번째 단계  
 ⇒ Client가 통신을 위해 임의의 Port 번호를 포함한 SYN 정보를 전송하는 단계에서의  
**Option 정보**

⇒ 이전 분석에서 Option이 등장하지 않아 추가  
 분석 진행

Option 부분	의미
Maximum segment size	- Maximum Segment size의 크기(65495): 송&수신 간에 가장 큰 Segment의 크기는 65495 - Kind(2) : <b>MSS의 옵션이 있음</b> 을 알려줌 - Length(4): <b>MSS 옵션이 차지하는 길이가 4</b>
Sack Permitted	- kind(4): Stack 옵션이 있음을 알려줌(송&수신 Host간의 Stack을 지원 가능 / 재전송할 패킷 만을 재전송할 수 있게 해주는 옵션) - Length(2): <b>Stack permitted 옵션이 차지하는 길이가 2</b>
Window Scale	- Window Scale(shift count: 8): - Kind(3): Window scale 정보가 있음을 알려줌(TCP Header 의 window size 필드가 부족할 경우 크기를 증가) - Length: Window Scale 옵션이 차지하는 길이가 3
No-Operation(NOP)	- NOP 옵션: 필요할 경우 송신 측이 필드를 채우기 옵션(4Byte)

# TCP Segment

## [2] Hand Shaking 과정 / Option 정보 추가해 분석 진행

```
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  TCP Option - Maximum segment size: 65495 bytes
    Kind: Maximum Segment Size (2)
    Length: 4
    MSS Value: 65495
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - Window scale: 8 (multiply by 256)
    Kind: Window Scale (3)
    Length: 3
    Shift count: 8
    [Multiplier: 256]
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - No-Operation (NOP)
    Kind: No-Operation (1)
  TCP Option - SACK permitted
    Kind: SACK Permitted (4)
    Length: 2
```



```
0000 02 00 00 00 45 00 00 34 42 b8 40 00 80 06 00 00 .....E..4 B.@.....
0010 7f 00 00 01 7f 00 00 01 c8 6e 27 10 ba 26 5c 84 .....n'..&\.
0020 00 00 00 00 80 02 ff ff 70 c0 00 00 02 04 ff d7 .....p.....
0030 01 03 03 08 01 01 04 02 .....

```

Format 내용(Option)	실제 값	아래 표현(header)	대응 표현
Max-mum	2(segment size), 4(length), 65495(value)	02 04 ff d7	...
Window	3(scale), 3(length), 8(shift count)	03 03 08	...
SACK 정보	4(permitted), 2(length)	04 02	..
NOP	1(kind: no-operation)	01	.

- Hand Shaking 과정 中 첫번째 단계  
⇒ Client가 통신을 위해 임의의 Port 번호를 포함한 SYN 정보를 전송하는 단계에서의  
**Option 정보**

⇒ 이전 분석에서 Option이 등장하지 않아 추가  
분석 진행