★★★

컴퓨터네트워크 설계보고서

9팀 안윤빈 양현용 채윤원 한승훈

CONTENTS

01
설계 목표

RAW SOCKET 을 활용해 OS에 의해
자동 가공되는 캡슐화 된 패킷의 정보 출력

1

TCP, UDP, IP 헤더와 Application 계층의
HTTP, DNS, email, traceroute 데이터 출력

2

3

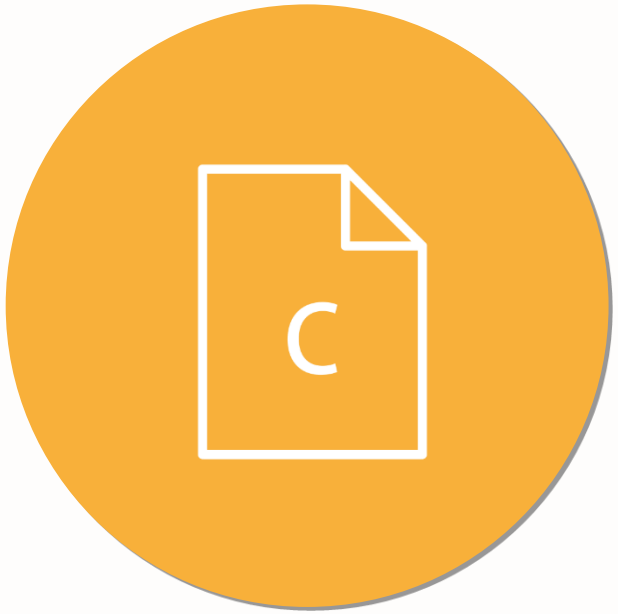
TCP 패킷의 TCP Flag를 출력하여
3-way Handshaking (연결)
4-way Handshaking (연결해제) 확인

4

올바른 결과를 확인하기 위해
Wireshark 프로그램과 비교함으로써
패킷 스니퍼의 동작 이해

02
설계 환경

Windows

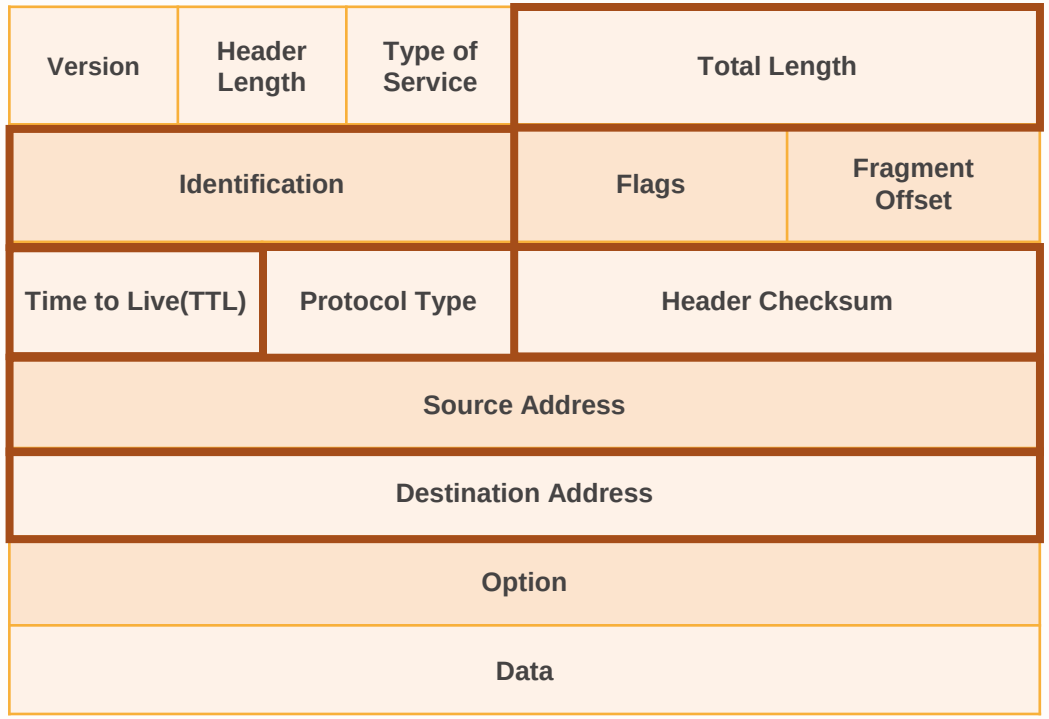


C language

PCAP Library

03
설계 내용 및 결과

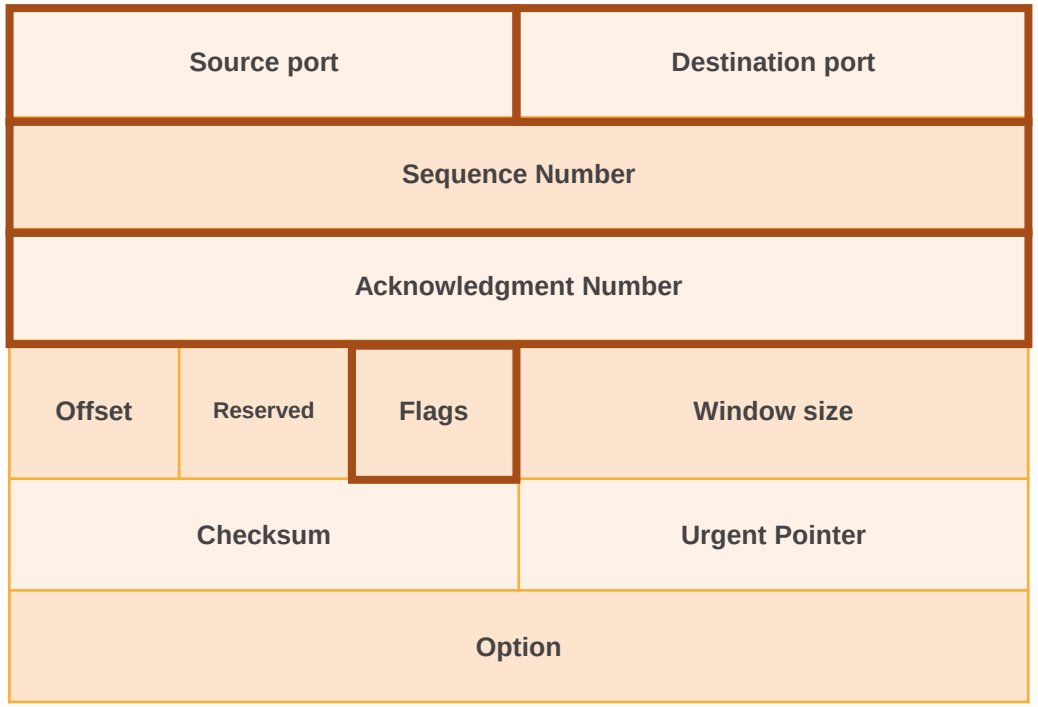
IP HEADER




```
typedef struct ip_hdr {
unsigned short ip_total_length;  // IP의 전체 길이
unsigned short ip_id;            // IP 고유 넘버
unsigned char ip_ttl;            // IP Time To Live
unsigned short ip_checksum;      // IP CheckSum
unsigned int ip_src_addr;        // 출발지의 IP주소
unsigned int ip_dest_addr;       // 도착지의 IP주소
}
```

03
설계 내용 및 결과

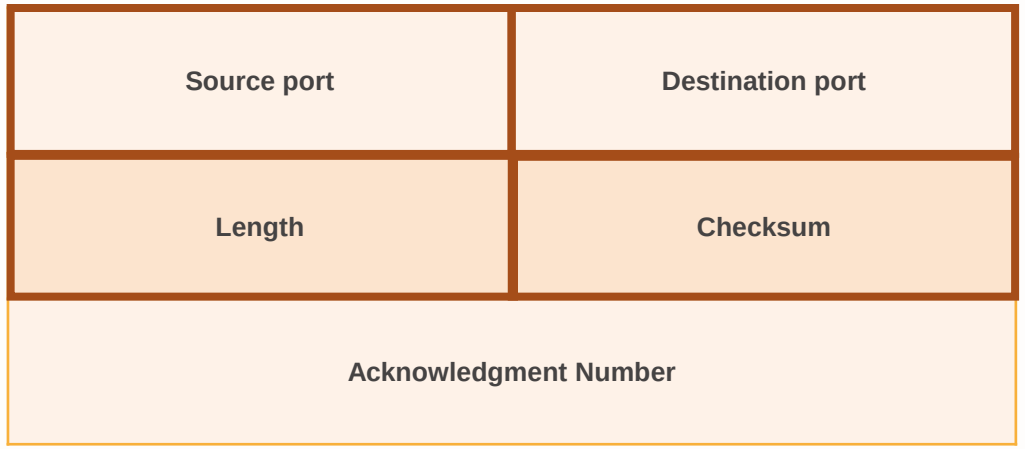
TCP HEADER




```
typedef struct tcp_hdr {
  unsigned short src_port;    // 출발지의 포트 번호
  unsigned short dest_port;     // 목적지의 포트 번호
  unsigned int sequence;        // SEQ
  unsigned int acknowledge;     // ACK
  unsigned char fin : 1, syn : 1, ack : 1;   // Flag 내부
}
```

03
설계 내용 및 결과

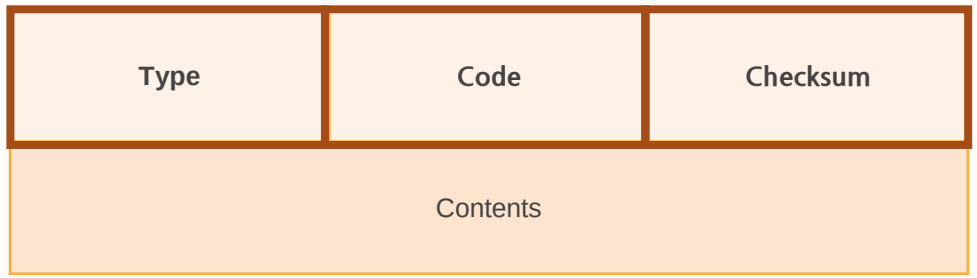
UDP HEADER




```
typedef struct udp_hdr {
 unsigned short src_port;          // 출발지 포트 번호
 unsigned short dest_port;         // 목적지 포트 번호
 unsigned short udp_length;        // UDP Datagram 길이
 unsigned short udp_checksum;      // UDP Checksum
}
```

03
설계 내용 및 결과

ICMP HEADER




```
typedef struct icmp_hdr {
  byte icmp_type;              // ICMP Error type
  byte icmp_code;              // Type sub code
  unsigned short checksum;     // ICMP Checksum
  unsigned short id;           // ICMP id
  unsigned short seq;          // ICMP SEQ
}
```

03

설계 내용 및 결과

HTTP

eclass.kpu.ac.kr

GET POST

DNS

portal.kpu.ac.kr

```
< UDP : 23 || Total : 58 >
**************************************************
 IP Header-------------------------------------------
 |  Source IP : 192.168.22.197
 |  Destination IP : 168.126.63.1
 |  IP Length : 62 Bytes(Size of Packet)
 |  IP inherence Num : 57849
 |  TTL : 128
 |  CheckSum : 39368
 ----------------------------------------------------


-----------------------------UDP Packet-----------------------------
 UDP Header------------------------------------------
 | Sourcer Port No. : 52828
 | Destination Port No. : 53
 | UDP Length : 42
 | UDP CheckSum : 11452
 ----------------------------------------------------

DNS Data Payload
    37 D3 01 00 00 01 00 00 00 00 00 00 06 70 6F 72          7............por
    74 61 6C 03 6B 70 75 02 61 63 02 6B 72 00 00 01          tal.kpu.ac.kr...
    00 01                                                    ..
```

nslookup

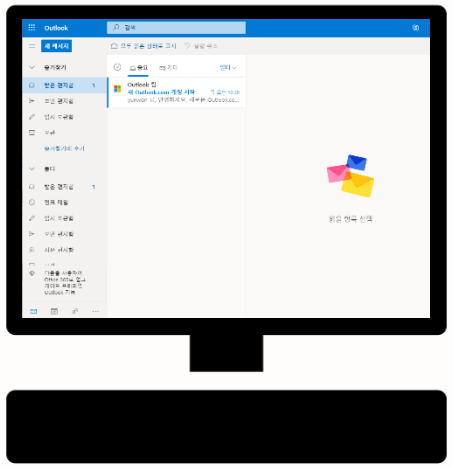
```
C:₩Users₩yunwon>nslookup 168.126.63.1
서버:    kns.kornet.net
Address:  168.126.63.1

이름:    kns.kornet.net
Address:  168.126.63.1
```

'패스 코리아 넷' 확인 결과
=> KT 네트워크 망

03

설계 내용 및 결과

EMAIL



outlook.com

[Gmail 사용]

IMAP SMTP

```
< TCP : 72 || Total : 82 >
**************************************************
IP Header----------
|  Source IP : 192.168.22.197
|  Destination IP : 64.233.189.109
|  IP Length : 80 Bytes(Size of Packet)
|  IP inherence Num : 19680
|  TTL : 128
|  CheckSum : 55299
---------------------------

-------------------------TCP Packet---
TCP Header----------
| Source Port No. : 62157
| Destination Port No. : 993
| SEQ No. : 2451809773
| ACK No. : 2192457037
| TCP Length : 20
| TCP CheckSum : 1565851648
TCP Flags----------
| SYN : 0
| ACK : 1
| FIN : 0
---------------------------------------------------

IMAP(SSL Security) Data Payload
    17 03 03 00 23 00 00 00 00 00 00 00 8C FA E3 45        ....#.........E
    81 AC 76 DE 15 79 10 A7 CF 06 E9 9B DA 66 AA 23        ..v..y.......f.#
    7F 2A 0F F2 0A 72 E9 23                                □*...r.#
```

64.233.189.109

```
{} asn: Object
  asn: "AS15169"
  name: "Google LLC"
  domain: "google.com"
  route: "64.233.189.0/24"
  type: "business"
{} hosting: Object
  host: "google"
```

ipinfo.io

```
< TCP : 12 || Total : 14 >
**************************************************
IP Header----------
|  Source IP : 192.168.22.197
|  Destination IP : 74.125.204.109
|  IP Length : 316 Bytes(Size of Packet)
|  IP inherence Num : 28242
|  TTL : 128
|  CheckSum : 40209
---------------------------

-------------------------TCP Packet---
TCP Header----------
| Source Port No. : 62358
| Destination Port No. : 465
| SEQ No. : 2809288315
| ACK No. : 566745165
| TCP Length : 20
| TCP CheckSum : 3693805568
TCP Flags----------
| SYN : 0
| ACK : 1
| FIN : 0
---------------------------------------------------

SMTP(SSL Security) Data Payload
    17 03 03 01 0F 00 00 00 00 00 00 02 FE 43 3B        .............C;
    1E 6C 42 7E 7C 2D 68 D5 FC 4D 01 43 04 AF 8A 45     .lB~|-h..M.C...E
    A5 9F 28 30 D9 7E 57 FE B5 AA 85 C5 AC 6D 44 57     ..(0.~W.....mDW
    21 26 94 09 4E 8E C4 5E 6A 92 54 0A 5E 9B 57 97     !&..N..^j.T.^.W.
    85 7F 73 BC AD EA 76 A6 0A 8F C6 A5 E2 D3 B2 D5     .□s...v.........
    8A DE F9 BC 32 A7 22 8C 83 FC D7 50 3B 60 30 E3     ....2."....P;`0.
    D7 B8 E4 2A 4B F8 8E 10 DF 04 EC 76 5C C1 D3 08     ...*K......v₩...
    1D 62 32 26 8D 20 74 50 24 07 48 DA 68 80 23 A3     .b2&. tP$.H.h□#.
    0E 4B 61 7B 0D 00 ED B3 72 58 9C 20 D0 32 1A 7C     .Ka{....rX. .2.|
    FD 8F 34 9D 3B FF 8B BF 82 04 9D C5 C9 7F EF 10     ..4.;.........□..
    4C 30 AA 93 6E 5A BF B0 13 49 C5 D5 0F CA B4 DD     L0..nZ...I......
    58 BC 05 04 C0 9D 80 8E 6F 0E 46 57 F4 37 B6 F2     X.....□o.FW.7..
    80 36 43 02 56 96 59 99 8C CB 08 21 ED 86 88 65     □6C.V.Y....!...e
    CE 7D FF 37 6A 72 F3 BC B1 36 B1 80 5B E5 77 B5     .}.7jr...6.□[.w.
    32 D4 F6 5B B6 44 FF F9 18 DF 50 18 8D 18 38 33     2..[.D....P...83
    4D F5 CD 2C 2C 33 8B 43 42 3C AC 70 AE 73 66 00     M..,,3.CB<.p.sf.
    EE 06 77 D4 08 62 04 5D C0 6E 4D 03 CC 06 6A 8B     ..w..b.].nM...j.
    DF 5B F7 93                                         .[..
```

74.125.204.109

```
{} asn: Object
  asn: "AS15169"
  name: "Google LLC"
  domain: "google.com"
  route: "74.125.204.0/24"
  type: "business"
{} hosting: Object
  host: "google"
```

03

설계 내용 및 결과

Traceroute

```
IP Header
|  Source IP : 192.168.35.108
|  Destination IP : 210.93.48.51
|  IP Length : 92 Bytes(Size of Packet)
|  IP inherence Num : 52252
|  TTL : 1
|  CheckSum : 1760

ICMP Packet
ICMP Header
|  ICMP Type No. : 8   Type 8 : Echo
|  ICMP Code No. : 0
|  ICMP Checksum : 62787
|  ICMP ID : 1
|  ICMP Sequence : 699
```

```
IP Header
|  Source IP : 192.168.35.108
|  Destination IP : 210.93.48.51
|  IP Length : 92 Bytes(Size of Packet)
|  IP inherence Num : 52255
|  TTL : 2
|  CheckSum : 1501

ICMP Packet
ICMP Header
|  ICMP Type No. : 8
|  ICMP Code No. : 0
|  ICMP Checksum : 62784
|  ICMP ID : 1
|  ICMP Sequence : 702
```

```
IP Header
|  Source IP : 192.168.35.108
|  Destination IP : 210.93.48.51
|  IP Length : 92 Bytes(Size of Packet)
|  IP inherence Num : 52258
|  TTL : 3
|  CheckSum : 1242

ICMP Packet
ICMP Header
|  ICMP Type No. : 8
|  ICMP Code No. : 0
|  ICMP Checksum : 62781
|  ICMP ID : 1
|  ICMP Sequence : 705
```

www.kpu.ac.kr

```
IP Header
|  Source IP : 192.168.35.108
|  Destination IP : 210.93.48.51
|  IP Length : 92 Bytes(Size of Packet)
|  IP inherence Num : 52261
|  TTL : 4
|  CheckSum : 983

ICMP Packet
ICMP Header
|  ICMP Type No. : 8
|  ICMP Code No. : 0
|  ICMP Checksum : 62778
|  ICMP ID : 1
|  ICMP Sequence : 708
```

```
IP Header
|  Source IP : 192.168.0.1
|  Destination IP : 192.168.35.108
|  IP Length : 92 Bytes(Size of Packet)
|  IP inherence Num : 52264
|  TTL : 254
|  CheckSum : 724

ICMP Packet
ICMP Header
|  ICMP Type No. : 11   Type 11 && Code 0 : TTL Exceed
|  ICMP Code No. : 0
|  ICMP Checksum : 62775
|  ICMP ID : 1
|  ICMP Sequence : 711
```

TTL : 라우터를 거치는 횟수 또는 데이터가 도착하는데 걸리는 시간

위 캡쳐와 같이 **TTL값이 증가**하는 것은 시간 초과되어 응답이 없어, TTL을 하나씩 늘려가며 계속해서 Echo Msg를 보내는 과정의 ICMP 패킷 캡쳐

3 Way-HandShaking

SEQ, ACK 값의 증가를 통해
연결 시 패킷 정상 탐지 확인

```
< TCP : 49 || Total : 79 >
IP Header
|  Source IP : 192.168.22.197
|  Destination IP : 216.58.197.228
|  IP Length : 52 Bytes(Size of Packet)
|  IP inherence Num : 37036
|  TTL : 128
|  CheckSum : 62602
TCP Packet
TCP Header
| Source Port No. : 62635
| Destination Port No. : 443
| SEQ No. : 2202808587
| ACK No. : 0
| TCP Length : 32
| TCP CheckSum : 1406402560
SYN : 1
ACK : 0
FIN : 0
```

①SYN

```
< TCP : 50 || Total : 80 >
IP Header
|  Source IP : 216.58.197.228
|  Destination IP : 192.168.22.197
|  IP Length : 52 Bytes(Size of Packet)
|  IP inherence Num : 37036
|  TTL : 128
|  CheckSum : 62785
TCP Packet
TCP Header
| Source Port No. : 443
| Destination Port No. : 62635
| SEQ No. : 1105602085
| ACK No. : 2202808588
| TCP Length : 36
| TCP CheckSum : 1406402580
SYN : 1
ACK : 1
FIN : 0
```

ACK = SEQ(1) + 1

②SYN+ACK

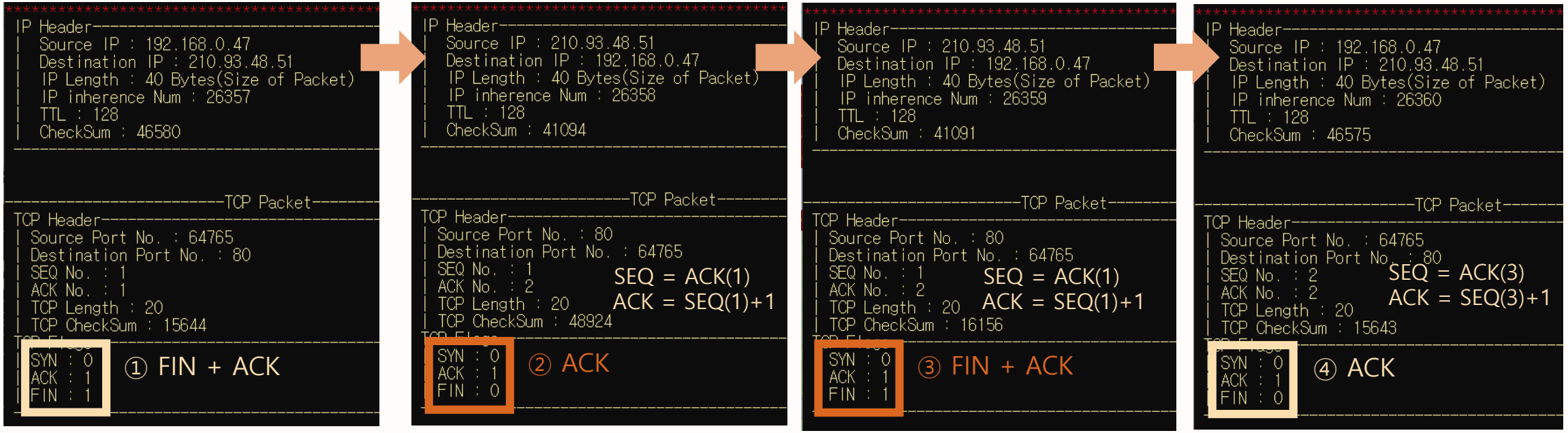
```
< TCP : 51 || Total : 81 >
IP Header
|  Source IP : 192.168.22.197
|  Destination IP : 216.58.197.228
|  IP Length : 56 Bytes(Size of Packet)
|  IP inherence Num : 37038
|  TTL : 128
|  CheckSum : 62874
TCP Packet
TCP Header
| Source Port No. : 62635
| Destination Port No. : 443
| SEQ No. : 1105602086
| ACK No. : 2202808589
| TCP Length : 40
| TCP CheckSum : 1406842406
SYN : 0
ACK : 1
FIN : 0
```

SEQ = SEQ(2) + 1
ACK = ACK(2) + 1

③ACK

4 Way-HandShaking

SEQ, ACK 값의 증가를 통해
연결 종료 시 패킷 정상 탐지
확인



4 Way-HandShaking

SEQ, ACK 값의 증가를 통해
연결 종료 시 패킷 정상 탐지
확인

37	12.801020	192.168.0.47	210.93.48.51	TCP	①	54 64765 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
38	12.801267	192.168.0.47	210.93.48.51	TCP		54 64768 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
39	12.801895	192.168.0.47	210.93.48.51	TCP		66 64772 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
40	12.802436	192.168.0.47	210.93.48.51	TCP		66 64773 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
41	12.805998	210.93.48.51	192.168.0.47	TCP	②	54 80 → 64765 [ACK] Seq=1 Ack=2 Win=32768 Len=0
42	12.807015	210.93.48.51	192.168.0.47	TCP		54 80 → 64768 [ACK] Seq=1 Ack=2 Win=32768 Len=0
43	12.807017	210.93.48.51	192.168.0.47	TCP		66 80 → 64772 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 SACK_PERM=1 WS=1
44	12.807220	192.168.0.47	210.93.48.51	TCP		54 64772 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
45	12.808134	210.93.48.51	192.168.0.47	TCP	③	54 80 → 64765 [FIN, ACK] Seq=1 Ack=2 Win=0 Len=0
46	12.808135	210.93.48.51	192.168.0.47	TCP		54 80 → 64768 [FIN, ACK] Seq=1 Ack=2 Win=0 Len=0
47	12.808255	192.168.0.47	210.93.48.51	TCP	④	54 64765 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0
48	12.808392	192.168.0.47	210.93.48.51	TCP		54 64768 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0

04
기대효과


캡처한 **패킷을 분석**하여 네트워크의 **프로토콜 동작원리를 이해**할 수 있다
TCP 연결과 연결해제 단계를 직접 분석하여 네트워크의 흐름을 파악할 수 있다
Wireshark 프로그램과 비교함으로써 패킷 스니퍼의 동작 원리를 이해할 수 있다.

Thank you