



컴퓨터네트워크 설계보고서

9팀 안윤빈 양현용 채윤원 한승훈



CONTENTS

- 01 설 계 목 표
- 02 설 계 환 경
- 03 설 계 내 용 및 결 과
- 04 기 대 효 과



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

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

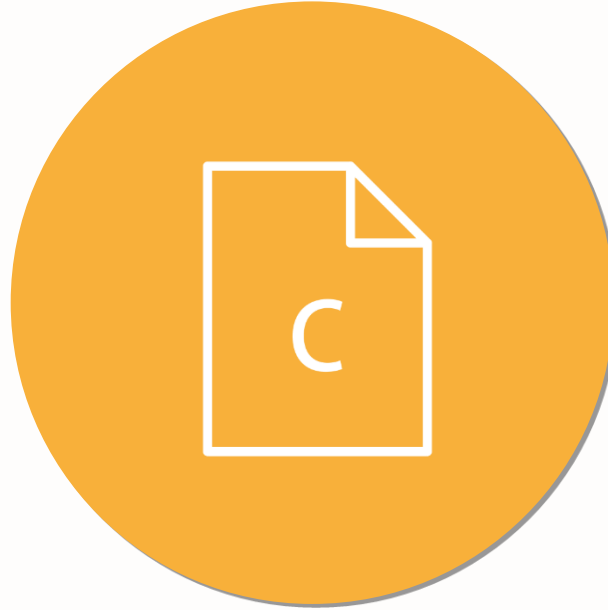
3

올바른 결과를 확인하기 위해
Wireshark 프로그램과 비교함으로써
패킷 스니퍼의 동작 이해

4



Windows



C language



PCAP Library



IP HEADER

Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live(TTL)	Protocol Type		Header Checksum	
Source Address				
Destination Address				
Option				
Data				

```
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
}
```



TCP HEADER

Source port			Destination port		
Sequence Number					
Acknowledgment Number					
Offset	Reserved	Flags	Window size		
Checksum			Urgent Pointer		
Option					

```
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
}
```



UDP HEADER

Source port	Destination port
Length	Checksum
Acknowledgment Number	

```
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  
}
```



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  
}
```


설계 내용 및 결과

HTTP



eclass.kpu.ac.kr

GET POST

```

*****
IP Header-----
| Source IP : 192.168.41.9
| Destination IP : 210.93.48.154
| IP Length : 695 Bytes(Size of Packet)
| IP inheritance Num : 20867
| TTL : 128
| CheckSum : 47636
-----

-----TCP Packet-----
TCP Header-----
| Source Port No. : 59924
| Destination Port No. : 80
| SEQ No. : 2037127594
| ACK No. : 3918444108
| TCP Length : 20
| TCP CheckSum : 244449280
-----
TCP Flags
| SYN : 0
| ACK : 1
| FIN : 0

요청 방식      웹서버 경로
GET /ilos/main/m
HTTP Data Payload
main_form.acl HTTP
P/1.1..Host: ecl
ass.kpu.ac.kr..C
onnection: keep
호스트

프로토콜 버전
GET /ilos/main/m
main_form.acl HTTP
P/1.1..Host: ecl
ass.kpu.ac.kr..C
onnection: keep
alive..Cache-Con
trol: max-age=0.
Upgrade-Insecur
e-Requests: 1..U
ser-Agent: Mozil
la/5.0 (Windows
NT 10.0; Win64;
x64) AppleWebKit
/537.36 (KHTML,
like Gecko) Chro
me/78.0.3904.108
Safari/537.36..
Accept: text/htm

```

```

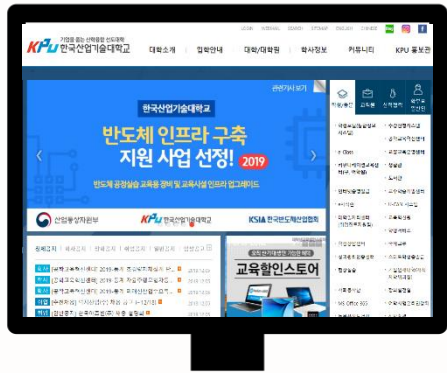
*****
IP Header-----
| Source IP : 192.168.41.9
| Destination IP : 210.93.48.154
| IP Length : 754 Bytes(Size of Packet)
| IP inheritance Num : 20883
| TTL : 128
| CheckSum : 47561
|-----

TCP Packet-----
TCP Header-----
| Source Port No. : 59924
| Destination Port No. : 80
| SEQ No. : 2037128249
| ACK No. : 3918490111
| TCP Length : 20
| TCP CheckSum : 762314752
|-----
TCP Flags-----
| SYN : 0
| ACK : 1
| FIN : 0

요청 방식      웹서버 경로
POST /ilos/main/quick_menu_list.
HTTP Data Payload: acf HTTP/1.1..Host: ec
                    st: eclass.kpu.ac.kr..Connection: keep-alive..Content-Length: 14..Accept: */*.Origin: http://eclass.kpu.ac.kr..X-Requested-With: XMLHttpRequest..User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
프로토콜 버전   호스트
61 63 6C 20 2F 2E 6F
73 74 3A 20
63 2E 6B 72
3A 20 6B 65
0E 74 65 6E 74 2D 4C 63 6E 67 74 68 3A 20 51 34
0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 4F
72 69 67 69 6E 3A 20 68 74 74 70 3A 2F 2F 65 63
6C 61 73 73 2E 6B 70 75 2E 61 63 2E 6B 72 0D 0A
58 2D 52 65 71 75 65 73 74 65 64 2D 57 69 74 68
3A 20 58 4D 4C 48 74 74 70 52 65 71 75 65 73 74
0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D 6F
74 69 6C 6C 61 2F 35 2E 30 28 57 69 6E 64 6F
77 73 20 4E 54 20 31 30 2E 30 3B 20 57 69 6E 36
34 3B 20 78 36 34 29 20 41 70 70 6C 65 57 65 62
4B 69 74 2F 35 33 37 2E 33 36 20 28 4B 48 54 4D
4C 2C 20 6C 69 6B 65 20 47 65 63 6B 6F 29 20 43
68 33 65 65 65 65 65 65 65 65 65 65 65 65 65

```

DNS



portal.kpu.ac.kr

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

```
< 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 inheritance Num : 57849
| TTL : 128
| CheckSum : 39368
|-----
```

UDP Packet

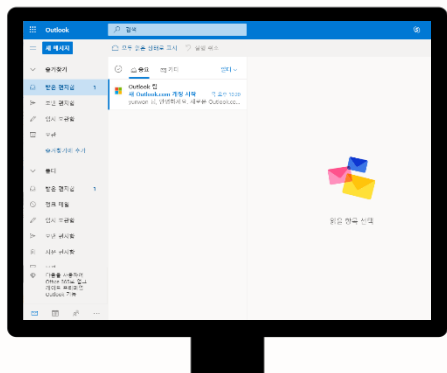
```
UDP Header-----
| Ssourcer Port No. : 52828
| Destination Port No. : 53
| UDP Length : 42
| UDP CheckSum : 11452
|-----
```

DNS Data Payload

```
37 D3 01 00 00 01 00 00 00 00 00 06 70 6F 72
74 61 6C 03 6B 70 75 02 61 63 02 6B 72 00 00 01
00 01
```

```
7.....por
tal.kpu.ac.kr...
..
```

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

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"

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 8C FA E3 45
 81 AC 76 DE 15 79 10 A7 CF 06 E9 9B DA 66 AA 23
 7F 2A 0F F2 0A 72 E9 23

.....#.....E
 ..v..y.....f.#
 0*...r.#

< 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

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"

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 02 FE 43 3B
 1E 6C 42 7E 7C 2D 68 D5 FC 4D 01 43 04 AF 8A 45
 A5 9F 28 30 D9 7E 57 FE B5 AA 85 C5 AC 6D 44 57
 21 26 94 09 4E 8E C4 5E 6A 92 54 0A 5E 9B 57 97
 85 7F 73 BC AD EA 76 A6 0A 8F 06 A5 E2 D3 B2 D5
 8A DE F9 BC 32 A7 22 8C 83 FC D7 50 3B 60 30 E3
 D7 B8 E4 2A 4B F8 8E 10 DF 04 EC 76 5C C1 D3 08
 1D 62 32 26 8D 20 74 50 24 07 48 DA 68 80 23 A3
 0E 4B 61 7B 0D 00 ED B3 72 58 9C 20 D0 32 1A 7C
 FD 8F 34 9D 3B FF 8B BF 82 04 9D C5 C9 7F EF 10
 4C 30 AA 93 6E 5A BF B0 13 49 C5 D5 0F CA B4 DD
 58 BC 05 04 C0 9D 80 8E 6F 0E 46 57 F4 37 B6 F2
 80 36 43 02 56 96 59 99 8C CB 08 21 ED 86 88 65
 CE 7D FF 37 6A 72 F3 BC B1 36 B1 80 5B E5 77 B5
 32 D4 F6 5B B6 44 FF F9 18 DF 50 18 8D 18 38 33
 4D F5 CD 2C 2C 33 8B 43 42 3C AC 70 AE 73 66 00
 EE 06 77 D4 08 62 04 5D C0 6E 4D 03 CC 06 6A 8B
 DF 5B F7 93

.....C;
 .IB-|h..M.C...E
 ..(O.-W.....mDW
 !&..N..^J.T..W.
 .0s...v.....
2.....P: 0.
 ...*K.....v#...
 .b2&. tP\$.H.h[
 .Ka{...rX...2.1
 ..4.....0...
 L0..nZ...l...
 X...o.FW.7...
 [BC.V.Y.....e
 .}.7jr...6.□.w.
 2...[D...P...83
 M...3.CB<p.sf.
 ..w..b.]nM...j.
 [...

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



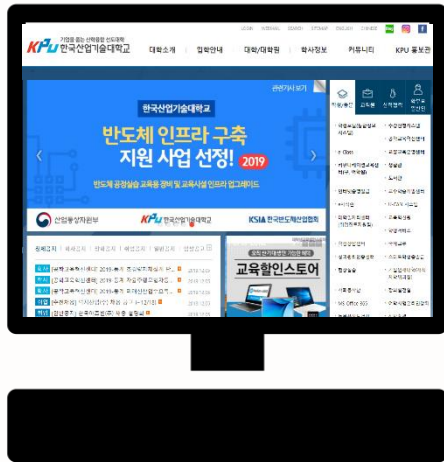
```

*****
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
    
```



```

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

www.kpu.ac.kr

TTL : 라우터를 거치는 횟수 또는 데이터가 도착하는데 걸리는 시간
위 캡처와 같이 **TTL값이 증가**하는 것은 시간 초과되어 응답이 없어, TTL을
하나씩 늘려가며 계속해서 Echo Msg를 보내는 과정의 ICMP 패킷 캡처



“ 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 inheritance 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
|-----|

TCP Flags-----
| SYN : 1
| ACK : 0
| FIN : 0
|-----|
  
```

① SYN

```

< 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 inheritance 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
|-----|

TCP Flags-----
| SYN : 1
| ACK : 1
| FIN : 0
|-----|
  
```

② SYN+ACK

ACK = SEQ(1) + 1

```

< 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 inheritance 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
|-----|

TCP Flags-----
| SYN : 0
| ACK : 1
| FIN : 0
|-----|
  
```

③ ACK

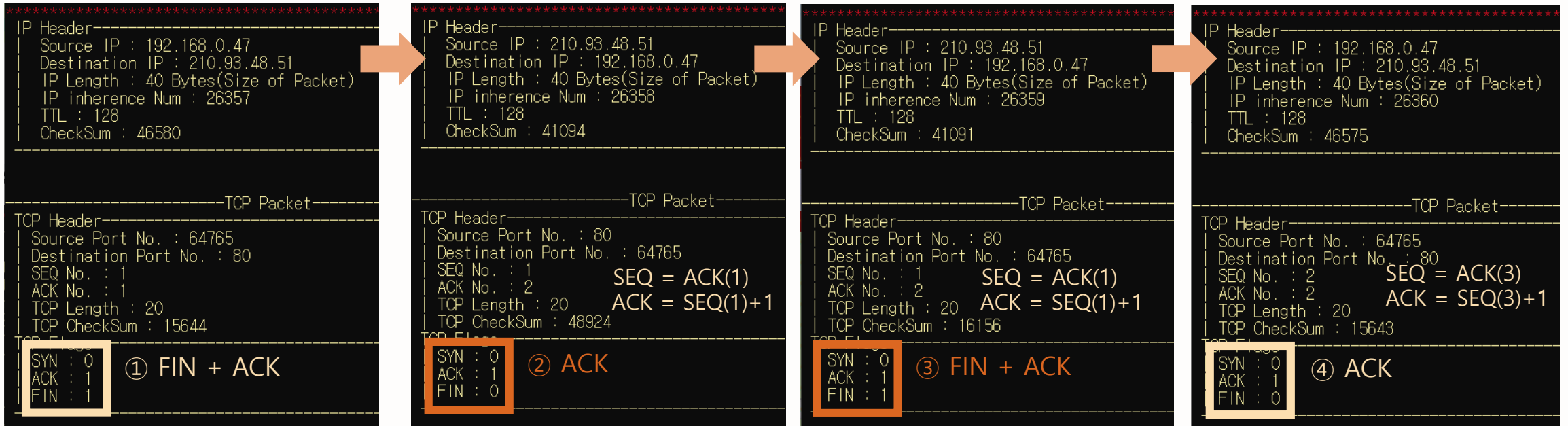
SEQ = SEQ(2) + 1
ACK = ACK(2) + 1



“ 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



캡처한 패킷을 분석하여 네트워크의 프로토콜 동작원리를 이해할 수 있다

TCP 연결과 연결해제
단계를 직접 분석하여
네트워크의 흐름을 파악
할 수 있다

Wireshark 프로그램과
비교함으로써 패킷 스니퍼의 동작 원리를 이해할 수 있다.



Thank you