PACC
2B01팀

강기덕,이동호,최형근

CONTENTS

Copyright©. Saebyeol Yu. All Rights Reserved.

Part 1.

제작동기

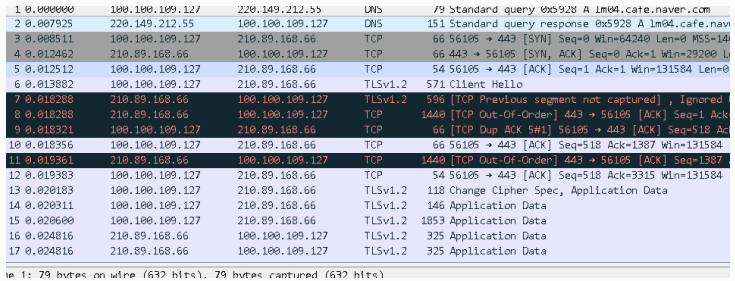
Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

1. 제작동기

현장 실습을 나가본 결과
장비끼리 통신이 안되어 **tcpdump**와 **wireshark**를
쓰게 되었는데 쉽지 않은 사용 방법 때문에 더 간단하게
패킷을 캡처할 수 있는 프로그램을 만들고 싶어
제안 하게 되었습니다.

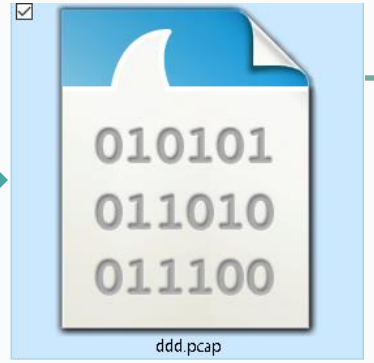
Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

1.2 사용한 프로그램 및 구조



1	0.000000	100.100.109.127	220.149.212.55	DNS	79 Standard query 0x5928 A lm04.cafe.naver.com
2	0.007925	220.149.212.55	100.100.109.127	DNS	151 Standard query response 0x5928 A lm04.cafe.nav
3	0.008511	100.100.109.127	210.89.168.66	TCP	66 56105 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=14
4	0.012462	210.89.168.66	100.100.109.127	TCP	66 443 → 56105 [SYN, ACK] Seq=0 Ack=1 Win=29200 L
5	0.012512	100.100.109.127	210.89.168.66	TCP	54 56105 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
6	0.013882	100.100.109.127	210.89.168.66	TLSv1.2	571 Client Hello
7	0.018288	210.89.168.66	100.100.109.127	TLSv1.2	596 [TCP Previous segment not captured] , Ignored
8	0.018288	210.89.168.66	100.100.109.127	TCP	1440 [TCP Out-Of-Order] 443 → 56105 [ACK] Seq=1 Ack
9	0.018321	100.100.109.127	210.89.168.66	TCP	66 [TCP Dup ACK 5#1] 56105 → 443 [ACK] Seq=518 Ac
10	0.018356	100.100.109.127	210.89.168.66	TCP	66 56105 → 443 [ACK] Seq=518 Ack=1387 Win=131584
11	0.019361	210.89.168.66	100.100.109.127	TCP	1440 [TCP Out-Of-Order] 443 → 56105 [ACK] Seq=1387
12	0.019383	100.100.109.127	210.89.168.66	TCP	54 56105 → 443 [ACK] Seq=518 Ack=3315 Win=131584
13	0.020183	100.100.109.127	210.89.168.66	TLSv1.2	118 Change Cipher Spec, Application Data
14	0.020311	100.100.109.127	210.89.168.66	TLSv1.2	146 Application Data
15	0.020600	100.100.109.127	210.89.168.66	TLSv1.2	1853 Application Data
16	0.024816	210.89.168.66	100.100.109.127	TLSv1.2	325 Application Data
17	0.024816	210.89.168.66	100.100.109.127	TLSv1.2	325 Application Data

e 1: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)



분석할 PCAP

입 , 출력

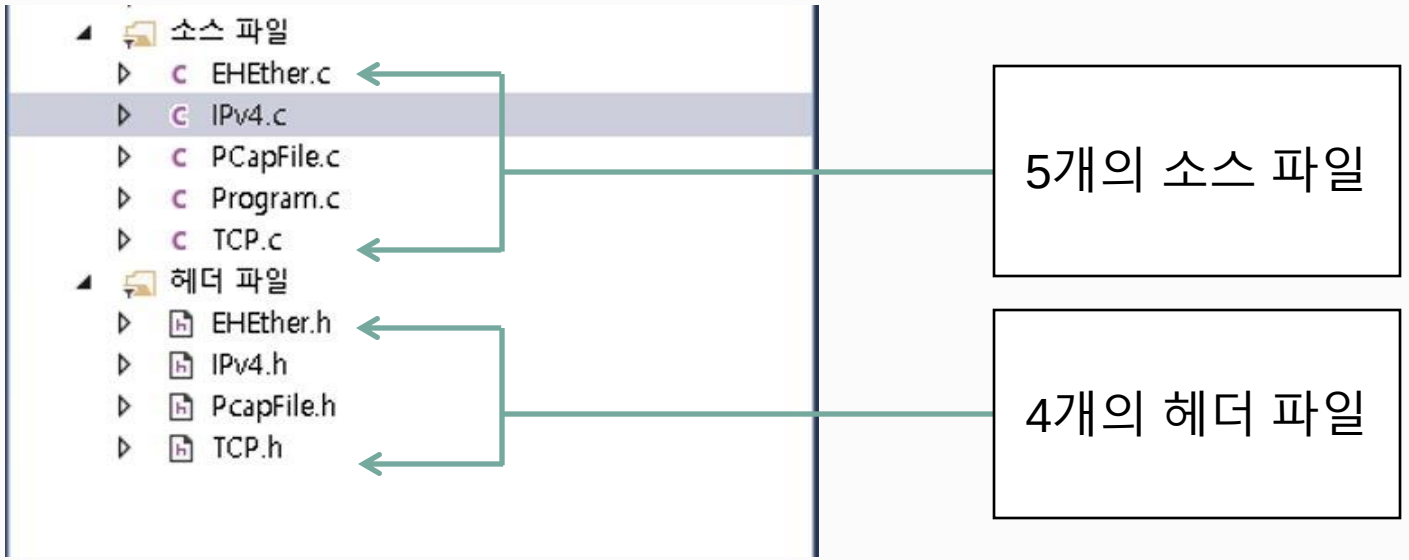
Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

Part 2.

전체 코드 설명

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

2. 전체 코드 설명



헤더 파일 – 변수
소스 파일 - 부분엔 함수와 각각의 출력 부분들이 있습니다.
대부분의 비교는 전역 변수를 이용하여 비교하였습니다.

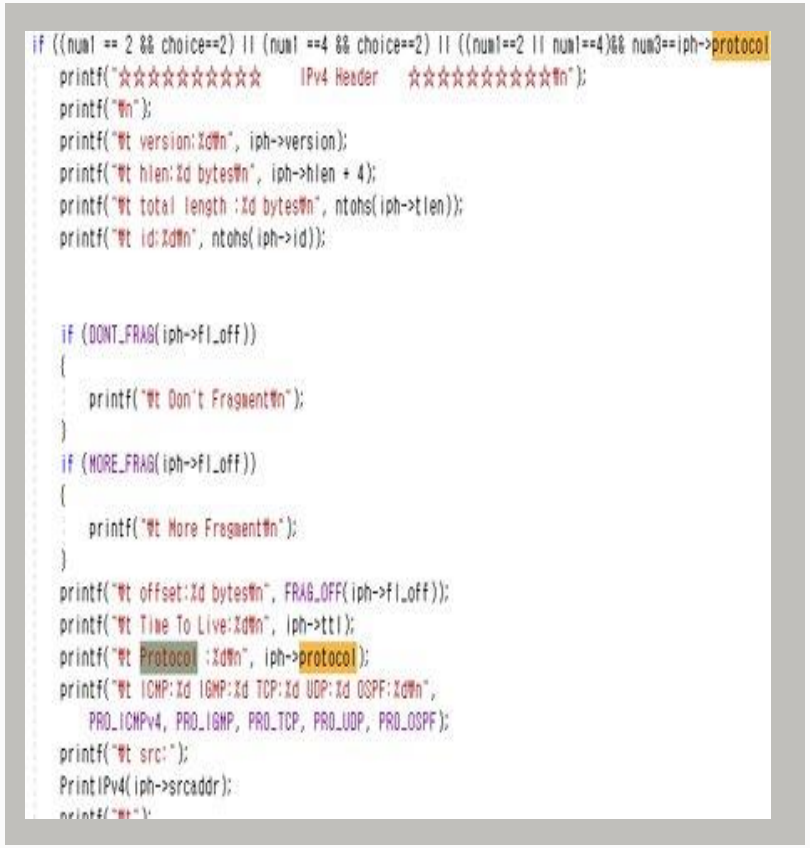
Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

Part 3.

옵션설명

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

3.1 3계층 옵션



```
if ((num1 == 2 && choice==2) || (num1 ==4 && choice==2) || ((num1==2 || num1==4)&& num3==iph->protocol
    printf("☆☆☆☆☆☆☆☆☆☆    IPv4 Header    ☆☆☆☆☆☆☆☆☆☆\n");
    printf("\n");
    printf("\t version:%d\n", iph->version);
    printf("\t hlen:%d bytes\n", iph->hlen * 4);
    printf("\t total length :%d bytes\n", ntohs(iph->tlen));
    printf("\t id:%d\n", ntohs(iph->id));


    if (DONT_FRAG(iph->fl_off))
    {
        printf("\t Don't Fragment\n");
    }
    if (MORE_FRAG(iph->fl_off))
    {
        printf("\t More Fragment\n");
    }
    printf("\t offset:%d bytes\n", FRAG_OFF(iph->fl_off));
    printf("\t Time To Live:%d\n", iph->ttl);
    printf("\t Protocol :%d\n", iph->protocol);
    printf("\t ICMP:%d IGMP:%d TCP:%d UDP:%d OSPF:%d\n",
        PRO_ICMPv4, PRO_IGMP, PRO_TCP, PRO_UDP, PRO_OSPF);
    printf("\t src:");
    PrintIPv4(iph->srcaddr);
```

*IP Protocol

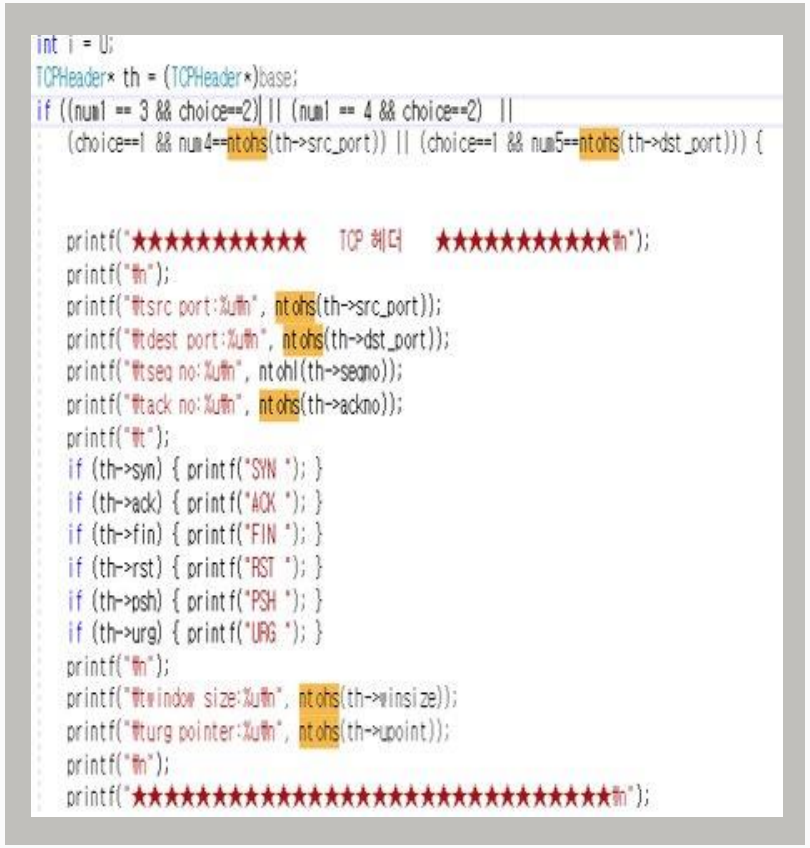
*TTL

-128 = window

-64 = linux

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

3.2 4계층 옵션



```
int i = 0;
TCPHeader* th = (TCPHeader*)base;
if ((num1 == 3 && choice==2) || (num1 == 4 && choice==2) ||
    (choice==1 && num4==ntohs(th->src_port)) || (choice==1 && num5==ntohs(th->dst_port))) {


    printf("★★★★★★★★★★★★  TCP 헤더  ★★★★★★★★★★★★\n");
    printf("\n");
    printf("\tsrc port:%u\n", ntohs(th->src_port));
    printf("\tdest port:%u\n", ntohs(th->dst_port));
    printf("\tseq no:%u\n", ntohl(th->seqno));
    printf("\tack no:%u\n", ntohs(th->ackno));
    printf("\t");
    if (th->syn) { printf("SYN "); }
    if (th->ack) { printf("ACK "); }
    if (th->fin) { printf("FIN "); }
    if (th->rst) { printf("RST "); }
    if (th->psh) { printf("PSH "); }
    if (th->urg) { printf("URG "); }
    printf("\n");
    printf("\twindow size:%u\n", ntohs(th->winsize));
    printf("\turg pointer:%u\n", ntohs(th->upoint));
    printf("\n");
    printf("★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★\n");
```

*SRC PORT NUM
출발지 포트
*DST PORT NUM
목적지 포트

Copyright©. Saebyeol Yu. All Rights Reserved.

Part 4.

실행확인

Copyright©. Saebyeol Yu. All Rights Reserved.

4.1 시작화면

PCAP파일의 주소 입력

설명에 따라 자신이 원하는 옵션을 설정 할 수 있습니다.

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

4.2 2계층

2계층 출력 부분입니다**.**

-목적지

-출발지

-L3type

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

4.3 3계층

3계층 출력 부분입니다.

-버전 -헤더길이

-ID **-Fragment**

-offset **-ttl**

-protocol **-src ip**

-dst ip

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

4.4 4계층

4계층 출력 부분입니다.

-Src Port -Sequence number

-Dst Port -Window Size

-Acknowledge number

-Flag

-Urgent Pointer

Copyrightⓒ. Saebyeol Yu. All Rights Reserved.

감사합니다

Copyright©. Saebyeol Yu. All Rights Reserved.