

Computer Network Term Project Report

49003157 최우석
f2sound@postech.ac.kr
010-6830-6360

설치 및 실행방법

Install

→ make all

Run

→ make run

*Remove *.out*

→ make clean

구현방법

1. pcap_findalldevs() 함수를 이용하여 모든 네트워크 인터페이스를 @alldevs에 저장한다.

```
if (pcap_findalldevs(&alldevs, errbuf) == -1) {  
    fprintf(stderr, "Error in pcap_findalldevs: %s\n", errbuf);  
    exit(1);  
}
```

2. 선택된 네트워크 인터페이스를 pcap_open_live() 를 이용하여 가져온다.

```
pcd = pcap_open_live(d->name, BUFSIZ, 1, 1000, errbuf);  
if (pcd == NULL) {  
    fprintf(stderr, "\nunable to open the adapter. %s is not supported\n", d->name);  
    /* Free the device list */  
    pcap_freealldevs(alldevs);  
    return -1;  
}  
else {  
    printf("\nselected device %s is available\n", d->description);  
}
```

3. pcap_loop() 를 이용하여 패킷을 캡처한다.

```
pcap_loop(pcd, -1, callback, NULL);
```

4. 들어오는 패킷에 대해 호출되는 callback() 함수는 다음과 같다.

```
void callback(u_char *param, const struct pcap_pkthdr *header, const u_char *pkt_data)
{
    struct ether_header *ehdr;
    unsigned short proto_type;

    // 이더넷 헤더
    ehdr = (struct ether_header *)pkt_data;

    // IP 헤더 (이더넷 헤더 크기만큼 offset)
    pkt_data += sizeof(struct ether_header);

    // 프로토콜 타입
    proto_type = ntohs(ehdr->ether_type);

    if (proto_type == ETHERTYPE_IP) { // IPv4
        struct ip *ip_hdr = (struct ip *)pkt_data;
        print_IPv4 (ip_hdr->ip_p, ip_hdr, (pkt_data + ip_hdr->ip_hl * 4));
    }
}
```

5. print_IPv4() 함수는 각 프로토콜에 맞는 출력을 수행한다.

```
void print_IPv4 (int PROTO_TYPE, struct ip* ip_hdr, void* proto_hdr) {
    if (PROTO_TYPE == IPPROTO_TCP) {
        printf ("%c[1;31m", 27);

        struct tcphdr *tcp_hdr = (struct tcphdr *)proto_hdr;
        _print_IPv4_time_and_mac_addr (ip_hdr);
        printf ("(%15s->%15s) TCP\t[port:%5d->%5d] [seq:%10u] [ack:%10u]",
            inet_ntoa(ip_hdr->ip_src),
            inet_ntoa(ip_hdr->ip_dst),
            ntohs(tcp_hdr->th_sport),
            ntohs(tcp_hdr->th_dport),
            tcp_hdr->th_seq,
            tcp_hdr->th_ack
        );

        printf ("%c[0m\n", 27);
    }
    else if (PROTO_TYPE == IPPROTO_UDP) {
```

6. MAC 주소를 호출하기 위한 함수의 원형은 다음과 같다. @ehdr->ether_shost 와 @ehdr->ether_dhost 를 형식에 맞게 출력한다.

```
void _print_IPv4_time_and_mac_addr (struct ether_header *ehdr) {
```

실행화면

```
root@wooseokyourself-B450M-DS3H:/home/wooseokyourself/simple_packet_capture# ./a.out
1. enp4s0 (No description available)
2. any (Pseudo-device that captures on all interfaces)
3. lo (No description available)
4. docker0 (No description available)
5. nflog (Linux netfilter log (NFLOG) interface)
6. nfqueue (Linux netfilter queue (NFQUEUE) interface)
7. usbmon1 (USB bus number 1)
8. usbmon2 (USB bus number 2)
9. usbmon3 (USB bus number 3)
10. usbmon4 (USB bus number 4)
11. usbmon5 (USB bus number 5)
12. usbmon6 (USB bus number 6)
Enter the interface number (1-12):1

selected device (null) is available
0.000061: [40:00:40:06:C1:88->45:00:00:34:03:F0]( 192.168.0.7-> 192.168.0.7) TCP [port:39456-> 80][seq: 111382123][ack:3741049357]
0.000095: [40:00:40:06:AD:9C->45:00:00:34:7E:5D]( 192.168.0.7-> 192.168.0.7) TCP [port:56192-> 443][seq:1107714984][ack:3817127749]
0.000105: [40:00:40:06:05:F7->45:00:00:34:A7:C2]( 192.168.0.7-> 192.168.0.7) TCP [port:49236-> 443][seq:1763801532][ack:1413639304]
0.000112: [00:00:78:06:5B:AE->45:00:00:34:5A:08]( 172.217.31.130-> 172.217.31.130) TCP [port: 443->49236][seq:1413639304][ack:1780578748]
0.000120: [00:00:78:06:C8:86->45:00:00:34:6B:73]( 172.217.161.65-> 172.217.161.65) TCP [port: 443->56192][seq:3817127749][ack:1124492200]
0.000134: [00:00:78:06:99:A1->45:00:00:34:33:D7]( 216.58.220.97-> 216.58.220.97) TCP [port: 80->39456][seq:3741049357][ack: 128159339]
0.000180: [40:00:40:06:CD:EE->45:00:00:34:DF:9E]( 192.168.0.7-> 192.168.0.7) TCP [port:60108-> 443][seq: 643755561][ack:2165968821]
0.000212: [00:00:78:06:DC:B2->45:00:00:34:D8:DA]( 172.217.31.174-> 172.217.31.174) TCP [port: 443->60108][seq:2165968821][ack: 660532777]
0.000221: [40:00:40:06:EC:B3->45:00:00:34:C6:84]( 192.168.0.7-> 192.168.0.7) TCP [port:36960-> 443][seq: 987123344][ack:3073889311]
0.000228: [40:00:40:06:C3:61->45:00:00:34:F1:58]( 192.168.0.7-> 192.168.0.7) TCP [port:33608-> 443][seq:1882845007][ack:1832695635]
0.000235: [00:00:78:06:3C:B0->45:00:00:34:80:0A]( 172.217.24.129-> 172.217.24.129) TCP [port: 443->33608][seq:1832695635][ack:1899622223]

0.007158: [00:00:78:06:72:08->45:00:01:AF:42:31]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:1614593080][ack: 3188816]
0.007169: [40:00:40:06:A3:57->45:00:00:34:0A:60]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack:3678256184]
0.007180: [00:00:78:06:6F:44->45:00:04:75:42:32]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:3678256184][ack: 3188816]
0.007193: [40:00:40:06:A3:56->45:00:00:34:0A:61]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack: 474135608]
0.007205: [00:00:78:06:DE:A0->45:00:00:7B:DD:D2]( 172.217.24.129-> 172.217.24.129) TCP [port: 443->33608][seq:2487007059][ack:3980128079]
0.007217: [40:00:40:06:C3:5D->45:00:00:34:F1:5C]( 192.168.0.7-> 192.168.0.7) TCP [port:33608-> 443][seq:3980128079][ack:3678189395]
0.007229: [00:00:78:06:DA:30->45:00:04:EA:DD:D3]( 172.217.24.129-> 172.217.24.129) TCP [port: 443->33608][seq:3678189395][ack:3980128079]
0.007241: [40:00:40:06:C3:5C->45:00:00:34:F1:5D]( 192.168.0.7-> 192.168.0.7) TCP [port:33608-> 443][seq:3980128079][ack:2437003091]
0.007254: [00:00:78:06:DE:C6->45:00:00:53:DD:D4]( 172.217.24.129-> 172.217.24.129) TCP [port: 443->33608][seq:2437003091][ack:3980128079]
0.007266: [40:00:40:06:C3:5B->45:00:00:34:F1:5E]( 192.168.0.7-> 192.168.0.7) TCP [port:33608-> 443][seq:3980128079][ack:2957096787]
0.007279: [00:00:78:06:DE:BD->45:00:00:5B:DD:D5]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->33608][seq:2957096787][ack:3980128079]
0.007291: [40:00:40:06:C3:5A->45:00:00:34:F1:5F]( 192.168.0.7-> 192.168.0.7) TCP [port:33608-> 443][seq:3980128079][ack:3611408211]
0.007303: [40:00:40:06:C3:32->45:00:00:5B:F1:60]( 192.168.0.7-> 192.168.0.7) TCP [port:33608-> 443][seq:3980128079][ack:3611408211]
0.007314: [00:00:78:06:6D:F9->45:00:05:BE:42:34]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq: 474135608][ack: 3188816]
0.007327: [40:00:40:06:A3:55->45:00:00:34:0A:62]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack:2789719096]
0.007338: [00:00:78:06:6D:F8->45:00:05:BE:42:35]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:2789719096][ack: 3188816]
0.007351: [40:00:40:06:A3:54->45:00:00:34:0A:63]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack: 810400824]
0.007363: [00:00:78:06:6D:F7->45:00:05:BE:42:36]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq: 810400824][ack: 3188816]
0.007374: [40:00:40:06:A3:53->45:00:00:34:0A:64]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack:3125984312]
0.007385: [00:00:78:06:6D:F6->45:00:05:BE:42:37]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:3125984312][ack: 3188816]
0.007397: [40:00:40:06:A3:52->45:00:00:34:0A:65]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack:1146666040]
0.007408: [00:00:78:06:71:25->45:00:02:8E:42:38]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:1146666040][ack: 3188816]
0.007420: [40:00:40:06:A3:51->45:00:00:34:0A:66]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack:2656746552]
0.007431: [40:00:40:11:AC:91->45:00:00:48:57:35]( 192.168.0.7-> 192.168.0.7) UDP [port:51263-> 53]
0.007442: [40:00:40:11:AC:8B->45:00:00:4D:57:36]( 192.168.0.7-> 192.168.0.7) UDP [port:47444-> 53]
0.007452: [40:00:40:11:AC:8A->45:00:00:4D:57:37]( 192.168.0.7-> 192.168.0.7) UDP [port:58995-> 53]
0.007462: [40:00:F9:11:C2:EA->45:00:01:6A:86:B9]( 210.220.163.82-> 210.220.163.82) UDP [port: 53->51263]
0.007472: [40:00:40:06:CB:18->45:00:03:00:DF:A5]( 192.168.0.7-> 192.168.0.7) TCP [port:60108-> 443][seq:1348464169][ack: 371265461]
0.007484: [40:00:40:11:AC:86->45:00:00:4E:57:3A]( 192.168.0.7-> 192.168.0.7) UDP [port:41344-> 53]
0.007495: [40:00:F9:11:6A:4F->45:00:00:7C:E0:42]( 210.220.163.82-> 210.220.163.82) UDP [port: 53->58995]
0.007506: [40:00:F9:11:83:43->45:00:00:79:C7:51]( 210.220.163.82-> 210.220.163.82) UDP [port: 53->47444]
0.007517: [40:00:40:11:AC:89->45:00:00:4A:57:3B]( 192.168.0.7-> 192.168.0.7) UDP [port:33524-> 53]
0.007527: [40:00:40:11:AC:85->45:00:00:4D:57:3C]( 192.168.0.7-> 192.168.0.7) UDP [port:46588-> 53]
0.007538: [40:00:F9:11:F3:20->45:00:00:5D:57:90]( 210.220.163.82-> 210.220.163.82) UDP [port: 53->46588]
0.007549: [40:00:F9:11:BA:ED->45:00:00:87:8F:99]( 210.220.163.82-> 210.220.163.82) UDP [port: 53->41344]
0.007560: [40:00:F9:11:F2:FD->45:00:00:7E:57:92]( 210.220.163.82-> 210.220.163.82) UDP [port: 53->33524]
0.007571: [40:00:40:06:73:89->45:00:00:3C:41:20]( 192.168.0.7-> 192.168.0.7) TCP [port:35496-> 443][seq:3409292379][ack: 0]
0.007583: [40:00:40:06:A1:D1->45:00:01:83:0A:67]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq: 3188816][ack:2656746552]
0.007595: [40:00:40:06:B1:43->45:00:00:3C:14:28]( 192.168.0.7-> 192.168.0.7) TCP [port:36160-> 443][seq:2638868792][ack: 0]
0.007607: [00:00:78:06:DE:CE->45:00:00:34:DD:D9]( 172.217.24.129-> 172.217.24.129) TCP [port: 443->33608][seq:3611408211][ack: 339537743]
0.007619: [00:00:78:06:6D:CF->45:00:05:BE:42:5F]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:2656746552][ack: 3188816]
0.007631: [40:00:40:06:A3:4F->45:00:00:34:0A:68]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq:2133960784][ack: 677428280]
0.007643: [00:00:78:06:6D:CD->45:00:05:BE:42:60]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq: 677428280][ack: 3188816]
0.007654: [40:00:40:06:A3:4E->45:00:00:34:0A:69]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq:2133960784][ack:2993011768]
0.007666: [00:00:78:06:6D:CC->45:00:05:BE:42:61]( 172.217.31.132-> 172.217.31.132) TCP [port: 443->35444][seq:2993011768][ack: 3188816]
0.007678: [40:00:40:06:A3:4D->45:00:00:34:0A:6A]( 192.168.0.7-> 192.168.0.7) TCP [port:35444-> 443][seq:2133960784][ack:1013693496]
```

```
Term — bash — 150x55
0.721450: [40:00:33:06:30:22->45:00:05:DC:8E:B3]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61257][seq:3604441993][ack:1132140472]
0.721461: [40:00:33:06:30:21->45:00:05:DC:8E:B4]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61257][seq:2128440201][ack:1132140472]
0.721472: [40:00:33:06:30:F4->45:00:05:08:8E:B5]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61257][seq: 652438409][ack:1132140472]
0.721485: [40:00:40:06:87:7D->45:00:00:34:00:00](211.251.238.160->211.251.238.160) TCP [port:61257-> 443][seq:1132140472][ack:2128440201]
0.721496: [40:00:40:06:87:7D->45:00:00:34:00:00](211.251.238.160->211.251.238.160) TCP [port:61257-> 443][seq:1132140472][ack:4226247561]
0.721507: [40:00:40:06:87:7D->45:00:00:34:00:00](211.251.238.160->211.251.238.160) TCP [port:61257-> 443][seq:1132140472][ack:4226247561]
0.721519: [40:00:39:11:24:52->45:00:00:35:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->57786]
0.721530: [40:00:40:06:87:7D->45:00:00:34:00:00](211.251.238.160->211.251.238.160) TCP [port:61257-> 443][seq:1132140472][ack:4226247561]
0.721541: [40:00:33:06:67:53->45:00:00:34:5D:2A]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61257][seq:4226247561][ack:1148917688]
0.721552: [40:00:39:11:32:F1->45:00:00:36:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721564: [40:00:39:11:31:D2->45:00:01:55:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721575: [40:00:39:11:32:EF->45:00:00:38:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721586: [00:00:40:11:53:4F->45:00:00:4E:18:8A]( 172.217.161.66-> 172.217.161.66) UDP [port:55539-> 443]
0.721597: [00:00:40:11:0A:B2->45:00:01:2E:51:A7](172.217.175.226->172.217.175.226) UDP [port:60454-> 443]
0.721608: [00:00:40:11:F1:CF->45:00:00:3D:7A:1A]( 172.217.161.66-> 172.217.161.66) UDP [port:55539-> 443]
0.721620: [40:00:39:11:24:52->45:00:00:35:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->60454]
0.721631: [40:00:39:11:32:F1->45:00:00:36:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721642: [40:00:39:11:23:A4->45:00:00:E3:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->60454]
0.721653: [40:00:39:11:24:50->45:00:00:37:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->60454]
0.721664: [00:00:40:11:BA:1B->45:00:00:3D:A3:2E](172.217.175.226->172.217.175.226) UDP [port:60454-> 443]
0.721676: [00:00:40:11:94:B2->45:00:00:47:C8:8D](172.217.175.226->172.217.175.226) UDP [port:60454-> 443]
0.721687: [00:00:40:11:79:87->45:00:00:EB:E3:14]( 172.217.175.226->172.217.175.226) UDP [port:57786-> 443]
0.721698: [40:00:40:06:1C:29->45:00:00:02:47:00:00]( 172.217.175.4-> 172.217.175.4) TCP [port:60771-> 443][seq: 689514438][ack:3031342120]
0.721709: [40:00:39:11:24:52->45:00:00:35:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->60454]
0.721720: [40:00:39:11:24:52->45:00:00:35:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->57786]
0.721732: [40:00:39:11:23:A5->45:00:00:E4:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->57786]
0.721743: [40:00:39:11:24:50->45:00:00:37:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->57786]
0.721754: [00:00:40:11:3F:1B->45:00:00:40:1E:1F](172.217.175.226->172.217.175.226) UDP [port:57786-> 443]
0.721765: [00:00:40:11:43:08->45:00:00:DE:28:41]( 172.217.161.66-> 172.217.161.66) UDP [port:55539-> 443]
0.721776: [00:00:78:06:CB:0C->45:00:00:34:5B:2F]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->60771][seq:3031342120][ack:1008412614]
0.721788: [00:00:40:11:C7:3B->45:00:00:3D:96:0E](172.217.175.226->172.217.175.226) UDP [port:57786-> 443]
0.721798: [00:00:78:06:CA:B8->45:00:00:79:5B:3E]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->60771][seq:3031342120][ack:1008412614]
0.721810: [00:00:78:06:CA:D0->45:00:00:53:5B:3F]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->60771][seq:4188970024][ack:1008412614]
0.721822: [00:00:78:06:CA:D4->45:00:00:5B:5B:40]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->60771][seq: 414161960][ack:1008412614]
0.721833: [40:00:40:06:1E:3C->45:00:00:34:00:00]( 172.217.175.4-> 172.217.175.4) TCP [port:60771-> 443][seq:1008412614][ack:4188970024]
0.721844: [40:00:40:06:1E:3C->45:00:00:34:00:00]( 172.217.175.4-> 172.217.175.4) TCP [port:60771-> 443][seq:1008412614][ack: 414161960]
0.721855: [40:00:40:06:1E:3C->45:00:00:34:00:00]( 172.217.175.4-> 172.217.175.4) TCP [port:60771-> 443][seq:1008412614][ack:1068473384]
0.721867: [40:00:40:06:1E:15->45:00:00:5B:00:00]( 172.217.175.4-> 172.217.175.4) TCP [port:60771-> 443][seq:1008412614][ack:1068473384]
0.721879: [40:00:39:11:24:52->45:00:00:35:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->57786]
0.721889: [40:00:39:11:32:F1->45:00:00:36:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721901: [00:00:78:06:CA:EB->45:00:00:34:5B:50]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->60771][seq:1068473384][ack:1662724038]
0.721912: [40:00:39:11:32:D1->45:00:00:56:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721923: [40:00:39:11:32:EF->45:00:00:38:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721934: [00:00:40:11:66:F2->45:00:00:4E:04:E7]( 172.217.161.66-> 172.217.161.66) UDP [port:55539-> 443]
0.721946: [40:00:39:11:32:F1->45:00:00:36:00:00]( 192.168.0.2-> 192.168.0.2) UDP [port: 443->55539]
0.721957: [40:00:36:06:3F:48->45:00:00:5B:6F:D6]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61137][seq:2140007670][ack:3924131458]
0.721968: [40:00:36:06:3F:56->45:00:00:4C:6F:D7]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61137][seq:2794319094][ack:3924131458]
0.721979: [40:00:40:06:A5:45->45:00:00:34:00:00]( 209.197.3.15-> 209.197.3.15) TCP [port:61137-> 443][seq:3924131458][ack:2794319094]
0.721991: [40:00:40:06:A5:45->45:00:00:34:00:00]( 209.197.3.15-> 209.197.3.15) TCP [port:61137-> 443][seq:3924131458][ack:3213749494]
0.722002: [40:00:40:06:A5:45->45:00:00:34:00:00]( 209.197.3.15-> 209.197.3.15) TCP [port:61137-> 443][seq:3924131458][ack:3213749494]
0.722013: [40:00:36:06:CE:C2->45:00:00:34:E0:82]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61137][seq:3213749494][ack:3940908674]
0.722024: [40:00:36:06:4F:7D->45:00:00:62:90:96]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61258][seq:2856997281][ack:3366038401]
0.722037: [40:00:36:06:4F:92->45:00:00:4C:90:97]( 192.168.0.2-> 192.168.0.2) TCP [port: 443->61258][seq:3628749217][ack:3366038401]
0.722048: [40:00:40:06:D6:41->45:00:00:34:00:00]( 210.117.209.98-> 210.117.209.98) TCP [port:61258-> 443][seq:3366038401][ack:3628749217]
0.722059: [40:00:40:06:D6:41->45:00:00:34:00:00]( 210.117.209.98-> 210.117.209.98) TCP [port:61258-> 443][seq:3366038401][ack:4048179617]
```

한 학기동안 감사했습니다.