\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Report: HW7

Author: F74071027 學貝萁 <youqing1211@gmail.com>

Class: 甲班

Description:

　　這次作業主要是拆解封包讀取裡面的資訊，並且需使用structure來儲存封包內的資訊。因為有助教給的範例程式碼所以好寫很多。感謝助教。

　　首先和之前一樣使用fopen和fread讀取檔案，然後使用structure來儲存封包內不同層的資訊（Ethernet、IPV4和TCP、UDP或ICMP），了解特定byte所儲存的資訊。當一個封包所需要的資訊都擷取完後，即將結果以特定格式輸出，之後while迴圈再次執行一次讀取下一個封包，直到檔案結束為止。結果可以看到封包使用哪種傳送方式、來源與目的的MAC位址、IP位址、Port等等資訊。

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Code:

#include<stdio.h>

#include<stdlib.h>

int Total = 0, TCP = 0, UDP = 0;

struct ethernet{

unsigned char DSTMAC[6];

unsigned char SRCMAC[6];

}Ethernet;

struct ipv4{

unsigned char TotalLength[2];

unsigned char Protocol[1];

unsigned char SRCIP[4];

unsigned char DSTIP[4];

}IPV4;

struct tcpudp{

unsigned char SRCPort[2];

unsigned char DSTPort[2];

}TCPUDP;

int main(int argc, char \*argv[]){

//open file=====

FILE \*rf;

rf = fopen(argv[1], "rb");

if(argc != 2 || rf == NULL){

printf("Error.\n");

return -1;

}

//==========

while(fread(Ethernet.DSTMAC, sizeof(char), 6, rf) != 0){

//read file=====

//MAC

fread(Ethernet.SRCMAC, sizeof(char), 6, rf);

//Length

fseek(rf, 4, SEEK\_CUR);

fread(IPV4.TotalLength, sizeof(char), 2, rf);

int Length = 256\*IPV4.TotalLength[0]+IPV4.TotalLength[1]+14;

//Protocol Type

fseek(rf, 5, SEEK\_CUR);

fread(IPV4.Protocol, sizeof(char), 1, rf);

//IP

fseek(rf, 2, SEEK\_CUR);

fread(IPV4.SRCIP, sizeof(char), 4, rf);

fread(IPV4.DSTIP, sizeof(char), 4, rf);

//Port: only TCP &UDP

if(IPV4.Protocol[0] == 6 || IPV4.Protocol[0] == 17){

if(IPV4.Protocol[0] == 6) TCP++;

else UDP++;

fread(TCPUDP.SRCPort, sizeof(char), 2, rf);

fread(TCPUDP.DSTPort, sizeof(char), 2, rf);

fseek(rf, Length-38, SEEK\_CUR);

}

else fseek(rf, Length-34, SEEK\_CUR);

//==========

//print out=====

Total++;

printf("#%d\n",Total);

printf("DST MAC: %02x:%02x:%02x:%02x:%02x:%02x\n", Ethernet.DSTMAC[0], Ethernet.DSTMAC[1], Ethernet.DSTMAC[2], Ethernet.DSTMAC[3], Ethernet.DSTMAC[4], Ethernet.DSTMAC[5]);

printf("SRC MAC: %02x:%02x:%02x:%02x:%02x:%02x\n", Ethernet.SRCMAC[0], Ethernet.SRCMAC[1], Ethernet.SRCMAC[2], Ethernet.SRCMAC[3], Ethernet.SRCMAC[4], Ethernet.SRCMAC[5]);

printf("Protocol: ");

if(IPV4.Protocol[0] == 6) printf("TCP\n");

else if(IPV4.Protocol[0] == 17) printf("UDP\n");

else printf("ICMP\n");

printf("SRC IP: %d.%d.%d.%d\n", IPV4.SRCIP[0], IPV4.SRCIP[1], IPV4.SRCIP[2], IPV4.SRCIP[3]);

printf("DST IP: %d.%d.%d.%d\n", IPV4.DSTIP[0], IPV4.DSTIP[1], IPV4.DSTIP[2], IPV4.DSTIP[3]);

if(IPV4.Protocol[0] == 6 || IPV4.Protocol[0] == 17){

printf("SRC Port: %d\n", 256\*TCPUDP.SRCPort[0]+TCPUDP.SRCPort[1]);

printf("DST Port: %d\n", 256\*TCPUDP.DSTPort[0]+TCPUDP.DSTPort[1]);

}

printf("Packet Length: %d\n\n", Length);

//==========

}

//

printf("Number of Packet: %d\n", Total);

printf("Number of TCP: %d\n", TCP);

printf("Number of UDP: %d\n", UDP);

printf("Number of ICMP: %d\n", Total-TCP-UDP);

fclose(rf);

return 0;

}

Compilation:

gcc hw7.c -o hw7

Execution:

./hw7 test.out

Output:

#1

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 66

#2

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63625

Packet Length: 66

#3

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 54

#4

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 104

#5

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63625

Packet Length: 54

#6

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 134

#7

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63625

Packet Length: 54

#8

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: UDP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 57229

DST Port: 80

Packet Length: 42

#9

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 164

#10

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63625

Packet Length: 54

#11

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 54

#12

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63625

Packet Length: 54

#13

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63625

DST Port: 80

Packet Length: 54

#14

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: ICMP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

Packet Length: 74

#15

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: ICMP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

Packet Length: 74

#16

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 66

#17

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63636

Packet Length: 66

#18

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 54

#19

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: UDP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 57229

DST Port: 5642

Packet Length: 69

#20

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: UDP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 57229

DST Port: 7890

Packet Length: 67

#21

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 106

#22

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63636

Packet Length: 54

#23

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 126

#24

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63636

Packet Length: 54

#25

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: UDP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 57229

DST Port: 7890

Packet Length: 67

#26

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 128

#27

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63636

Packet Length: 54

#28

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63636

Packet Length: 54

#29

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 54

#30

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: TCP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 63636

DST Port: 80

Packet Length: 54

#31

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: TCP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

SRC Port: 80

DST Port: 63636

Packet Length: 54

#32

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: UDP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 57229

DST Port: 7890

Packet Length: 67

#33

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: ICMP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

Packet Length: 74

#34

DST MAC: 08:62:66:50:b8:4e

SRC MAC: 00:08:9b:c4:61:fc

Protocol: ICMP

SRC IP: 140.116.82.171

DST IP: 140.116.82.165

Packet Length: 74

#35

DST MAC: 00:08:9b:c4:61:fc

SRC MAC: 08:62:66:50:b8:4e

Protocol: UDP

SRC IP: 140.116.82.165

DST IP: 140.116.82.171

SRC Port: 57229

DST Port: 1013

Packet Length: 61

Number of Packet: 35

Number of TCP: 25

Number of UDP: 6

Number of ICMP: 4