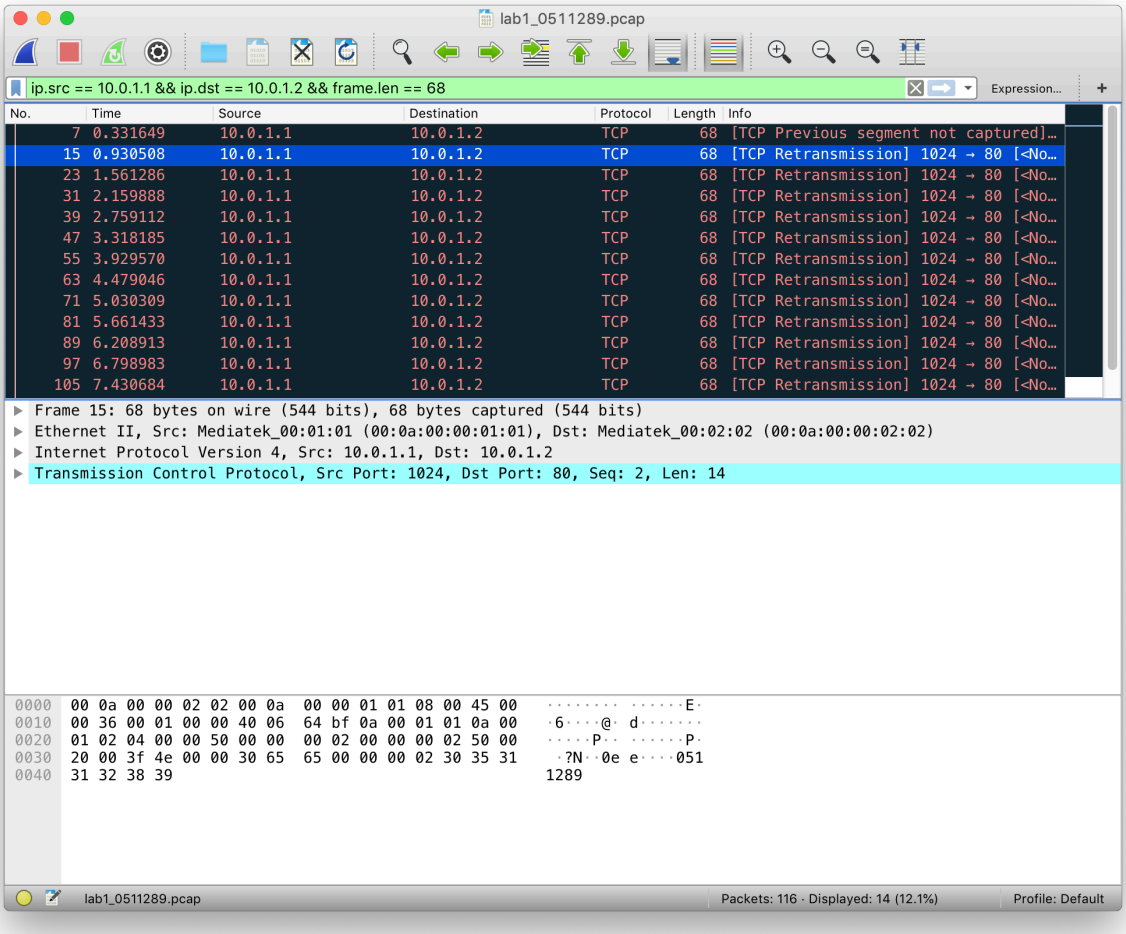
NCTU CN2018 Lab. 1- Packet Manipulation via Scapy

Student name: 邱宏明　　Student id: 0511289　　Department: EE

PartA. Questions

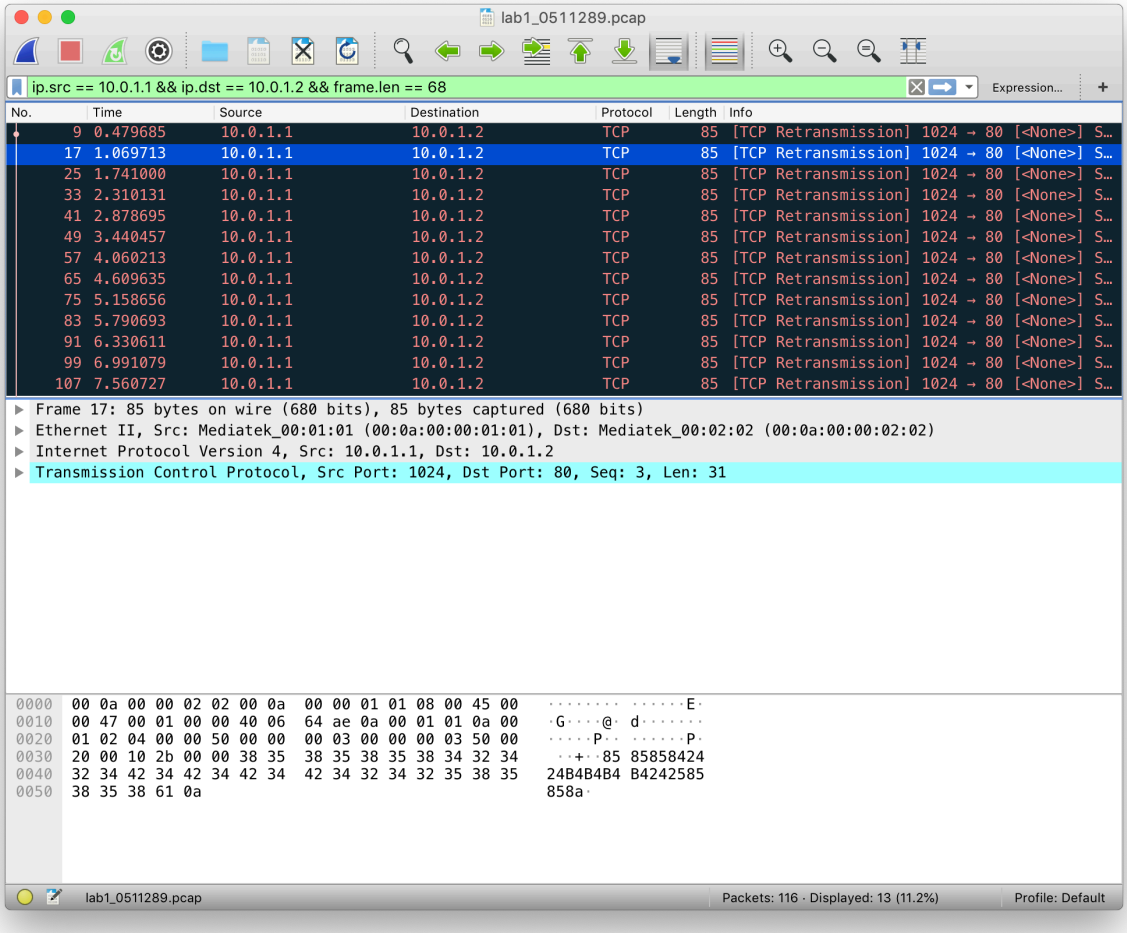
1. What is your command to filter the packet with customized header on Wireshark?
   I use “ip.src == 10.0.1.1 && ip.dst == 10.0.1.2 && frame.len == 68”

2. Show the screenshot of filtering the packet with customized header.



3. What is your command to filter the with “secret” payload on Wireshark?
   I use “ip.src == 10.0.1.1 && ip.dst == 10.0.1.2 && frame.len == 85”

4. Show the screenshot of filtering the packet with “secret” payload.



5. Show the result after decoding the “secret” payload
   98211509821150

PartB. Description

Task1. Environment setup

First clone the repository form TA’s GitHub account to my local machine directory and setup the remote url to make this directory become the master of my own GitHub account.

Then, setup the docker file for the purpose of building container later. In docker file, we first have to download the image file from TA and then install some package that will be used in the lab, in this case tcpdump and scapy, and then we have to specify which port we want to run our container, in this case 22. Finally, we have to clone the depository from TA’s GitHub account again so that the container will have the file we need for this lab as well.

After all these setting, because I am using Mac, I run main.sh to built the container then I ssh into the container I just built.

Task2. Define protocol via Scapy

This task is about define one kind of packet's header we want to send. We will send two kind of packet, the packer with custom header and the packet with secret payload, this one is the former one.

In this task, you just need to follow the syntax of Scapy to define your own protocol, for me, I define my custom header as follow, student = Hong-Ming, dept = ee, gender = male, id = 0511289.

Task3. Send packet

This task will focus on making a sender program which will send the packet for me. First we have to define the ip addresses and port of the source and destination and define my own customize header. Then we can start to send packets, we first build the TCP connection between source and destination by sending request and getting respond from destination, this part is done in ACK section, as you can see there is a flag 'A' in pocket meaning that this pocket is for sending the request.

After building the TCP connection between source and destination, we can start sending the pocket we want to send, first pocket is the pocket with custom header, as you can see int the code, there is a line "packet = ip / tcp / student" which mean my pocket's header will contain the information ip, tcp, and student (my custom header). The next pocket is similar to the previous one, but instead of sending custom header, we send secret payload, this secret payload is define by TA, base on my observation, I think TA has reversed my id and append the numbers in my id before each line of text in TA's file sequentially.

Task4. Sniff packet

This task will build a receiver for sniffing packets, this sniffer will sniff all the pockets send to this system, not only the pocket send from sender which we previously define. But how do we know we have receive the two kind of packet we have created? We can identify by looking the TCP seq, if seq = 2, which mean we get a pocket with custom header, if seq = 3, which mean we get a pocket with secret payload. While receiving the packets with secret payload, we will store the information and write to the output file after receiving process terminated.

Task5. Run sender and receiver

This task is about running the sender and receiver we just made, because the sender and receiver are all run in the same container, we have to use tmux, tmux stands for terminal multiplexer, which will allow us to open two pane, one for sender, another for receiver. Run the receiver first and then sender, you will see some packets be sniffed by receiver.

Task6. Push your file to remote

This task is just about push your task to your own GitHub account, I actually push my file every time I finish each task and I also writing some commit message to indicate what I have done.

Task7. Load PCAP via Wireshark

This is just open Wireshark and load the PCAP file.

Task8. Filter the target packet

There are a lot of packets after loading PCAP file, I use I use "ip.src == 10.0.1.1 && ip.dst == 10.0.1.2 && frame.len == 68" to filter out the pocket with custom header and I use "ip.src == 10.0.1.1 && ip.dst == 10.0.1.2 && frame.len == 85" to filter out the pocket with secret payload.

Task9. Decode the secret key

Run the decoder with secret key to get a Pokemon image, I get a blue Pokemon ball with very low resolution.

Bonus

What you have learned in this lab?

I have learned how to define your own protocol and sending, receiving pockets. Moreover, this is my first time using Wireshark, I have seen this on youtube video with someone trying to demonstrate how dangerous is using a public wifi by catching the pockets in the air and using Wireshark to filter out the pocket he want, then he can see some images, mails, messages, sent by some user who connected to public wifi.

This lab makes me understand how easy to sniff a pocket and how my personal information could be stolen when I connected to some public wifi or even cable. I hope that I could learn more about it in later course and how to prevent it as well.

What difficulty you have met in this lab?

First of all because I am using mac, I'm pretty familiar with terminal, thus this lab is not very hard for me. The main difficulty in this lab is to truly understand all the codes used in the lab, some are beyond the scope of my knowledge but I will trying to understand it.