实验报告 Lab 6

姓名：王钦　学号：13349112

Part I: Understanding minisniff

1. use pcap libaray.I can find more information on http://www.tcpdump.org/
2. Advantage

   easy to use

   compatible with other programs

   compatible with operat system both windows and linux

   capture all incoming and outgoing packets
3. Disadvantage

   writen on C language,not have python java etc. other language version.

   if dont have computer basic knowledge. it's difficult to learn.
4. Yes,I have searched on github and find some open source repositories like this one `https://github.com/AnwarMohamed/Packetyzer`
5. Explain functions(use man command on linux)

   `pcap_lookupdev` – find the default device on which to capture

   `pcap_open_live` – open a device for capturing

   `pcap_lookupnet` – find the IPv4 network number and netmask for a device

   `pcap_compile` – compile a filter expression

   `pcap_setfilter` – set the filter

   `pcap_next` – read the next packet from a `pcap_t`

   `pcap_loop` – process packets from a live capture or savefile

   `pcap_dispatch` – process packets from a live capture or savefile
6. on transport layer,because I can find some fields which only show in transport layer such as protocol and total length.

Part II: Extending minisniff

1. I modify some code in `capture.c` file see below

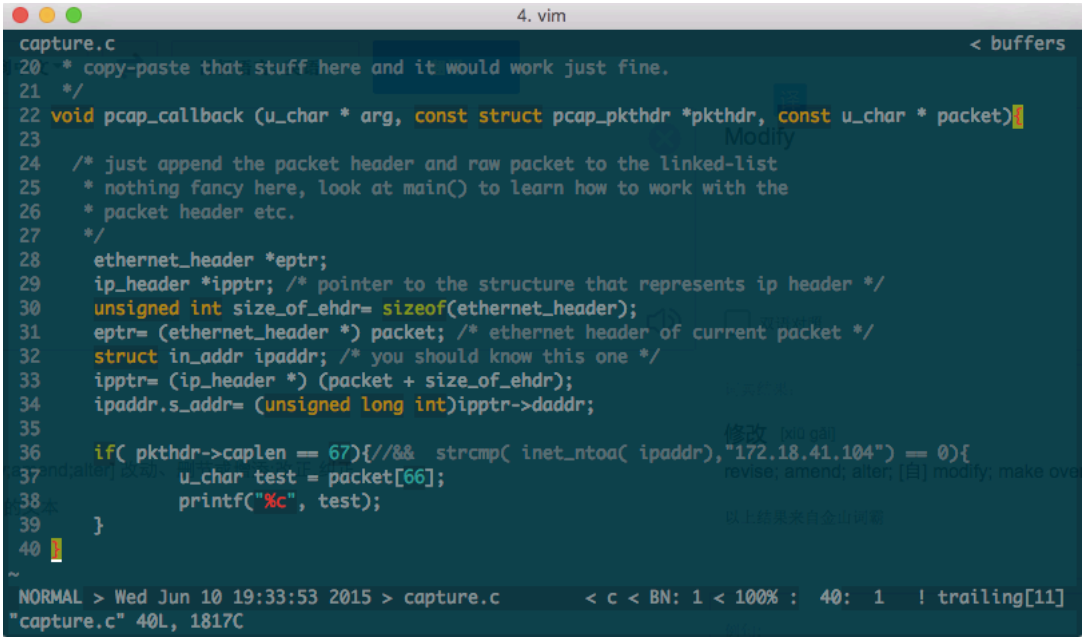

Figure 1: minisniff

2. screetshots see below ,all code is in minisniff folder.User is tsunami,password is 1. server is 172.18.187.113 linux which is my computer in Laboratory.I use macbook as clinet sent telnet to server.

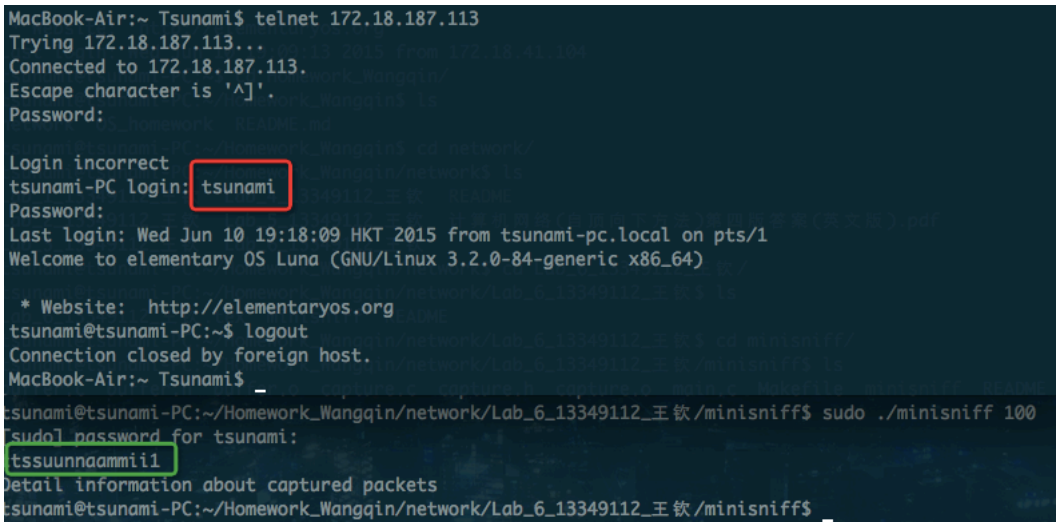

Figure 2: minisniff