SHRUTHI KATAPALLY
Username: shrukata

PROJECT-3 WIRETAP

INTRODUCTION:
This project parses the packet headers like Ethernet, IP, TCP. We parse the file and will get the information such as time stamp, Source and Destination ports, IP address, Ethernet address etc.

This project submission has the following things:

- wiretap.c
- Makefile
- Readme

1) **wiretap.c :**

   We parse the packets one by one and will print the information using the structures we from the headers included.

   We use the headers like Ethernet(#include<netinet/ether.h>),IP(#include <linux/ip.h>), TCP(#include <netinet/tcp.h>) and TLS(#include <time.h>,#include <limits.h>) are parsed to get the information like Source and Destination addresses, ports, Timestamp,etc.

   1) struct statistics –we used this to place all the variables for the counters purpose.
   2) Maps are used in this project to implement counters.
   3) void string_mac_address(const struct ether_addr *addr, char *address)—this gives us the MAC address of the packet
   4) void print_summary(struct statistics *stat) –this method gives us the summary such as timestamp, packet size, maximum, minimum and average packet size.
   5) void parse_packet(struct pcap_pkthdr *header, const unsigned char *pcap_packet, struct statistics *stat)—this method will parse the file which is taken as the input.

2) **Makefile:**
   A Makefile is written for the ease of compilation.The file wiretap.c is complied and an object file wiretap.o is generated using this makefile. It is also used for removing the previously generated object file.

3) **Readme:**
   Readme gives the description of the code for the program wiretap.c and the compilation procedure to execute the program. It also contains the output is analyzation.

References and Credits:

Project Partner:
Aliaksandr Krukau (akrukau)

Books:
1) http://www.tcpdump.org/pcap.htm

2) http://www.beej.us/guide/bgnet/

3) https://www.wireshark.org/

4) Reference for IPv4 is RFC 791. Reference for Ethernet frame format is: IEEE standard 802.3. http://standards.ieee.org/findstds/standard/802.3-2012.html. ICMP protocol is defined in: RFC 792