ASSIGNMENT 5

Problem Statement: Write a program for Log Capturing and Event Correlation.

OUTPUTS:

```
nikhil1771@nikhil1771:~$ cd Desktop/CSDF/
nikhil1771@nikhil1771:~/Desktop/CSDF$ gcc Logging.c && sudo ./a.out
Logging.c: In function ‘main’:
Logging.c:54:2: warning: implicit declaration of function ‘close’; did you mean
‘pclose’? [-Wimplicit-function-declaration]
   54 |  close(sock_raw);
      |  ^~~~~
      |  pclose
[sudo] password for nikhil1771:
Starting...
TCP : 746   UDP : 0   ICMP : 0   IGMP : 0   Others : 0   Total : 745
```

```
**********************TCP Packet**************************

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 44  Bytes(Size of Packet)
   |-Identification    : 374
   |-TTL      : 64
   |-Protocol : 6
   |-Checksum : 28042
   |-Source IP        : 34.107.221.82
   |-Destination IP   : 10.0.2.15

TCP Header
   |-Source Port      : 80
   |-Destination Port : 56100
   |-Sequence Number    : 39296001
   |-Acknowledge Number : 1728128873
   |-Header Length      : 6 DWORDS or 24 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 1
```

```
                        DATA Dump
IP Header
    45 00 00 2C 01 76 00 00 40 06 6D 8A 22 6B DD 52         E..,.v..@.m."k.R
    0A 00 02 0F                                             ....
TCP Header
    00 50 DB 24 02 57 9C 01 67 01 27 69 60 12 FF FF         .P.$.W..g.'i`...
    84 12 00 00 02 04 05 B4                                 ........
Data Payload

################################################################
```