Project Scope:

Introduction:   
This project is a software that is meant for networking purposes such as trace connections, view the contents of suspect network transactions and identify bursts of network traffic. **We are building a software that is a replication of a software called WireShark.**

What is WireShark:   
  
Wireshark is a network protocol analyzer, or an application that captures packets from a network connection.

Functionalities:   
we are looking to develop a similar software that can perform some WireShark functionalities, not all of them, only some.

The functionalities that we are looking for are:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

What this software is not:

This software does not have to be perfect, we only are looking for the main functionalities to work, such as the ones mentioned above like capturing packets and filtering them depending on the type of the packet and then giving a report of what have been captured from the network in that a span of time, but the software does not have to be graphical like wireShark, we are looking forward for the terminal output only, no need for a whole design.

What this Software is and will perform:

1. Sniff on an interface
2. Decode IP header and write it to the file or stdout
3. If Protocol is TCP/UDP/IGMP/ICMP; protocol specific headers are decoded
4. Statistics on the packet reception (Number of IP packets / sec, Number of TCP/UDP and other packets)