NS1

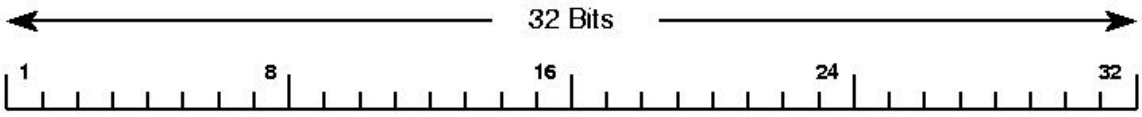
The program is composed of two blocks: Networking & Graphics. The Graphics block is divided in two files:

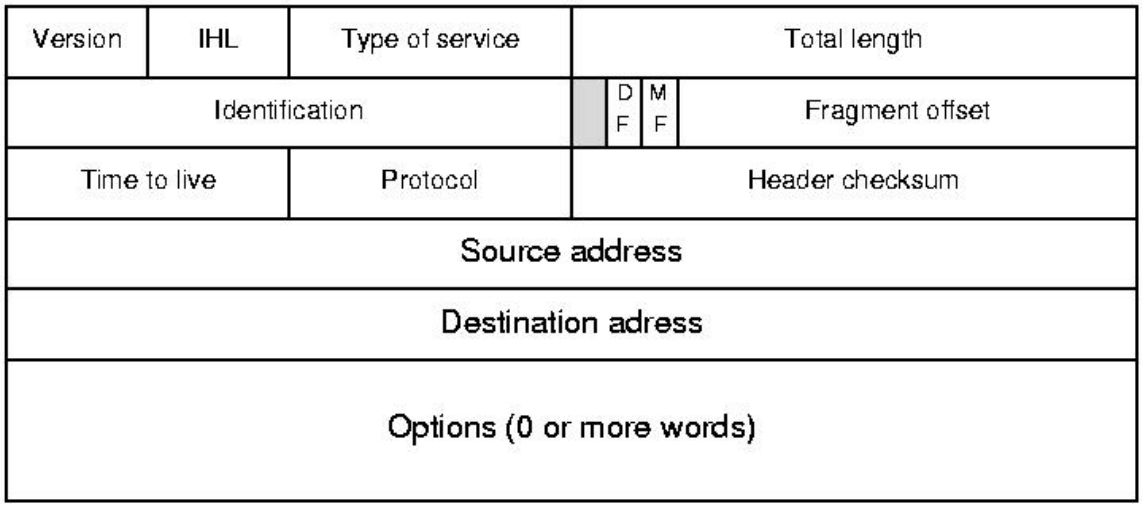
- GraphicWindow.cpp/.hpp which controls and produces the User Interface and commands
- GraphicWorker.cpp/.hpp which manages threads

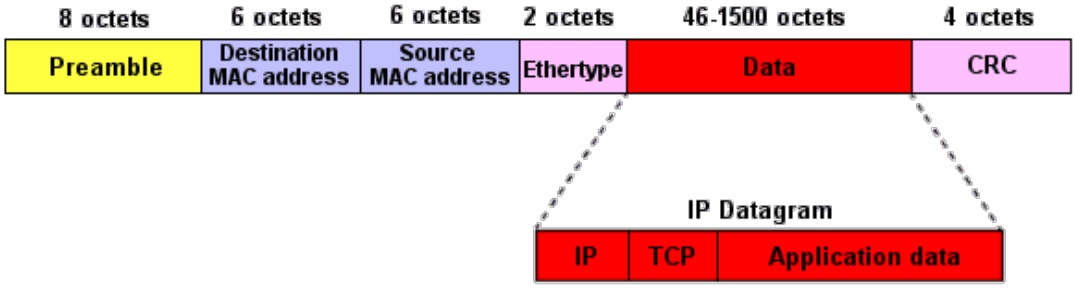
In the visual part of the program you will see caught packets and you will see their contents. Then we have LivePacketCapture.cpp/.hpp that contains the class with all the methods linked to the networking part of the project. This class contains methods to:

- Load / write / read a PCAP file
    - LivePacketCapture::Load/Write/Read
- Recognize packets from Ethernet / IP / ICMP / TCP / UDP
    - LivePacketCapture::ReadEthernet/IP/ICMP/TCP/UDP
- Capture from raw socket
    - LivePacketCapture::Capture

Thanks to raw sockets, we can capture any outgoing packets on the network. Raw sockets are available on network gear which makes it easy for us to tap in.
Here are a few header datagrams explaining how we parse the data and manage to read every format cited above:







TCP Segment Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags		Window Size			
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			