TEAM 403

Packet Sniffer

CSE 4344

Amado Jose

Johnny Tran

Ariel Widjaja

Aaqif Muhtasim

Omair Sunka

**Basic Functionality:**

The program uses a raw socket to catch Ethernet frames and the reads the content inside the said frames to determine the transport, network and application layer protocols encapsulated in it. It is able to read Link Layer – Ethernet Frames and ARP packets, Network Layer – IP and ICMP packets, Transport Layer – TCP and UDP and Application Layer – HTTP.

The code uses the information on the header of the previous layer to determine what the upper layer protocols are. The packets are then unpacked using the string format for their header and the information displayed as a string.

**GUI:**

A window opens with a start and stop button used to start and stop the sniffer. A console below the window then shows the content for each packet. A graph button opens the graph which shows the throughput per unit time for the sniffer as well as showing the average throughput.

**Libraries:**

import Tkinter

import time

import socket

import struct

import binascii

import matlibplot

**Other Info:**

The code was written on Python v2.7 and was implemented on Linux since windows does not allow access to Ethernet frames.