Kingdom of Saudi Arabia
Ministry of Education
University of Jeddah
College of Science and Computer Engineering

المملكة العربية السعودية
وزارة التعليم
جامعة جدة
كلية علوم و هندسة الحاسب

Computer Networks Lab Project:

Network Monitoring

Fadi Alzahrani	2240012
Ahmed Ammar	1845420
Faris Alghamdi	2040630
Abdulaziz Alasmari	2241335
Abdullah alkhairy	2241508

Supervised by: Dr. Majid Alghamdi

Table of Contents

Kingdom of Saudi Arabia
Ministry of Education
University of Jeddah
College of Science and Computer Engineering

جامعة جدة
University of Jeddah

المملكة العربية السعودية
وزارة التعليم
جامعة جدّة
كلية علوم و هندسة الحاسب

Introduction:

This program is a real time network monitoring tool used to analyze network traffic in real time and give numerical and graphical representations.

It utilizes **Scapy** library to track key metrics such as (Protocol Usage, Unique IP/Mac Address,Throughput,Latency, Packet Size) while logging packet details.

It runs the tasks concurrently using **Threads** and graphs the information as charts using **matplot** such as (Throughput over time, Latency distribution,Protocol Usage) and presents it stylishly with **colorama** in the console. It includes a signal handler for graceful termination allowing the user to terminate the program using **CTRL+C**

Project Outline:

Logging

- Analyze ethernet, IP, TCP and UDP statistics
- Timestamps for every log
- Number of the logs
- Unique IP and MAC

Calculations

- Calculate throughput in second
- Calculate latency in millisecond
- Calculate Throughput over time in minutes

Graphs

- Graph that shows the usage of Protocol
- Graph that shows Network throughput over time
- Graph that shows latency Distribution

Functions Used:

def initialize_metrics(self):to make sure the program is prepared to run properly,the function initializes key variables and metrics.

def initialize_throughput_tracking(self):the function sets up data structures to monitor ethernet,tcp,udp protocol speed and latency

def packet_callback(self, packet) :each message that is collected is processed by the method by extracting ethernet ,ip,tcp,and udp layer information

update _metrics method: is called at each packet captured and logs the event in the log and tracks the latency data for the packets

Calculate_throughput: this method calculates the throughput and prints the data to the console every 10 seconds

Display_statistics method: displays the data stats every 30 seconds

Print_current_stats: this prints the current networks stats to the console

Generate_visualizations: this method does all the graphs and aggregations of its data

Start_monitoring: this method creates two thread for display_stats and calculate_throuput

Stop_monitoring: this method prints the final stat and stops the capture be setting the exit_flag and exits

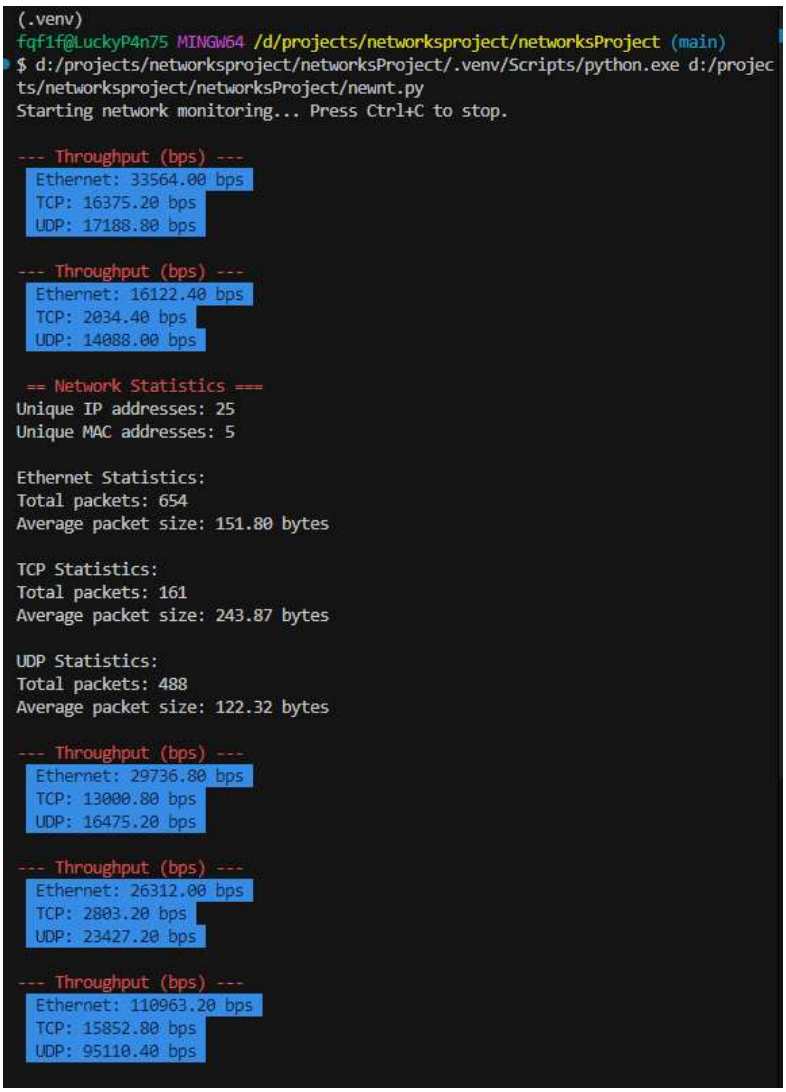
Signal_handler: this method prints a stop text and exits the program

Main function: to start the program

Results:

When running the program, scapy sniffed packets successfully. Texts were outputting as expected. And colored.

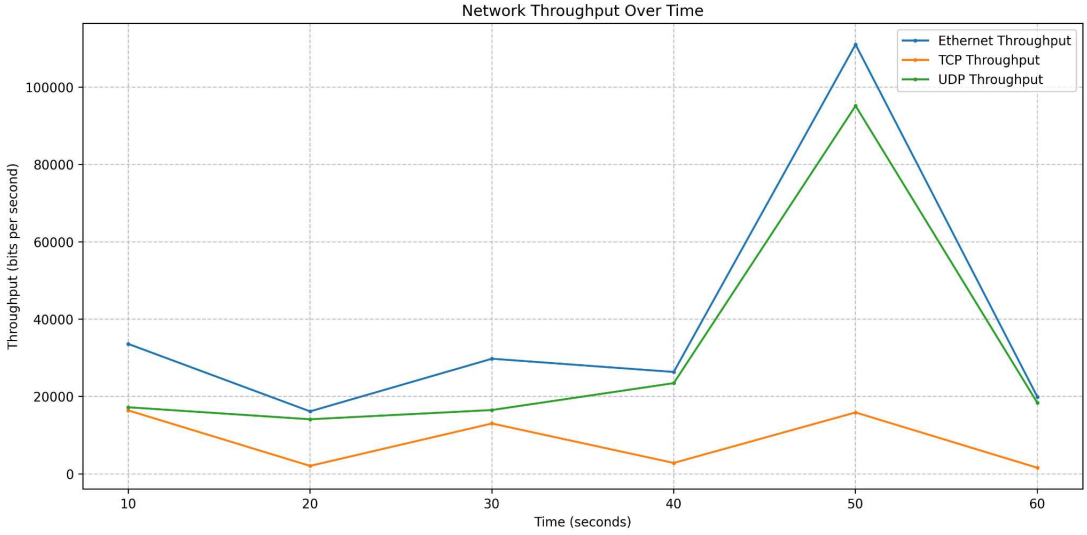
1: when the program is executed, it prints the throughput every 10 seconds and the stats every 30 seconds

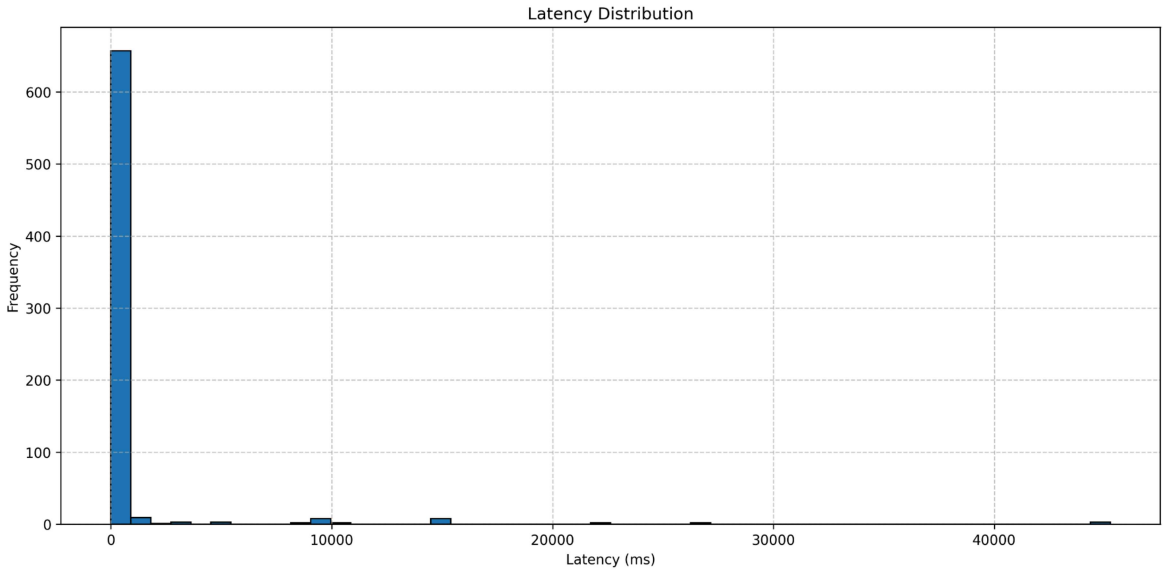


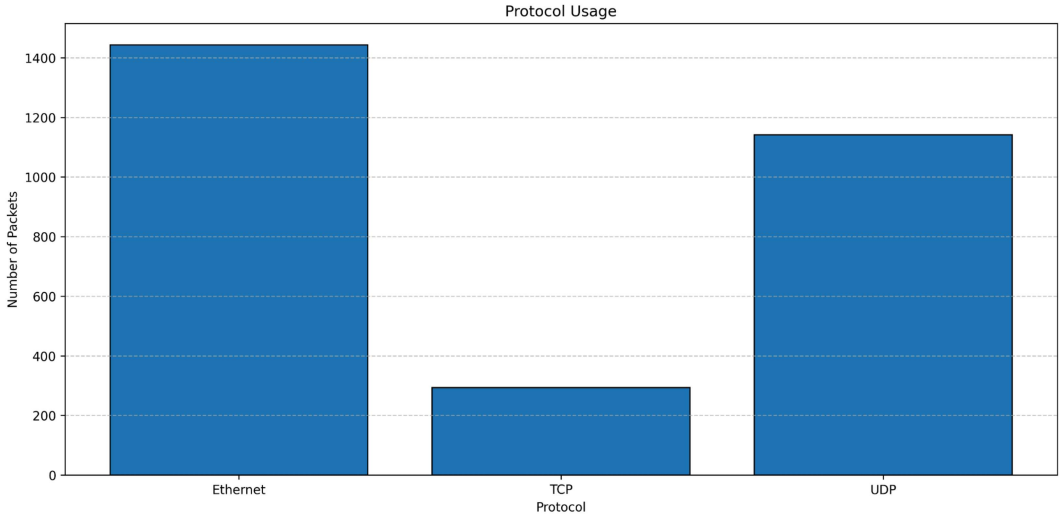
2.a final stat is printed after the user terminates the program

```
=== Final Statistics ===

 == Network Statistics ===
Unique IP addresses: 30
Unique MAC addresses: 5

Ethernet Statistics:
Total packets: 1443
Average packet size: 208.22 bytes

TCP Statistics:
Total packets: 294
Average packet size: 220.69 bytes

UDP Statistics:
```

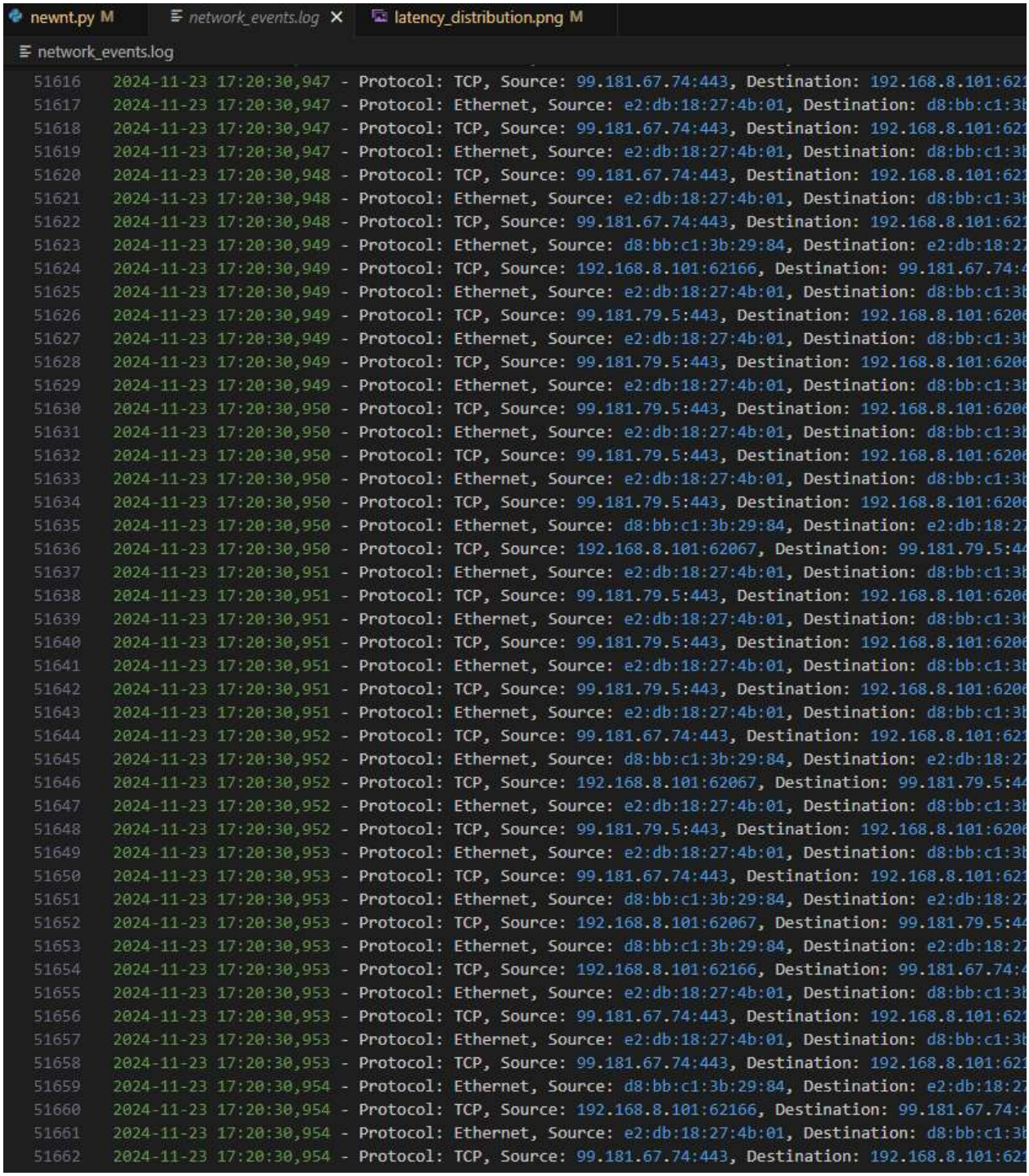
3. Graphs are created after the user termination:




Latency Distribution
Frequency
0
100
200
300
400
500
600
0
10000
20000
30000
40000
Latency (ms)


Protocol Usage
Number of Packets
0
200
400
600
800
1000
1200
1400
Ethernet
TCP
UDP
Protocol

4. Log file:


newnt.py M
network_events.log
latency_distribution.png M
network_events.log
51616 2024-11-23 17:20:30,947 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51617 2024-11-23 17:20:30,947 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51618 2024-11-23 17:20:30,947 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51619 2024-11-23 17:20:30,947 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51620 2024-11-23 17:20:30,948 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51621 2024-11-23 17:20:30,948 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51622 2024-11-23 17:20:30,948 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51623 2024-11-23 17:20:30,949 - Protocol: Ethernet, Source: d8:bb:c1:3b:29:84, Destination: e2:db:18:27
51624 2024-11-23 17:20:30,949 - Protocol: TCP, Source: 192.168.8.101:62166, Destination: 99.181.67.74:4
51625 2024-11-23 17:20:30,949 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51626 2024-11-23 17:20:30,949 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51627 2024-11-23 17:20:30,949 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51628 2024-11-23 17:20:30,949 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51629 2024-11-23 17:20:30,949 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51630 2024-11-23 17:20:30,950 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51631 2024-11-23 17:20:30,950 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51632 2024-11-23 17:20:30,950 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51633 2024-11-23 17:20:30,950 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51634 2024-11-23 17:20:30,950 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51635 2024-11-23 17:20:30,950 - Protocol: Ethernet, Source: d8:bb:c1:3b:29:84, Destination: e2:db:18:27
51636 2024-11-23 17:20:30,950 - Protocol: TCP, Source: 192.168.8.101:62067, Destination: 99.181.79.5:44
51637 2024-11-23 17:20:30,951 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51638 2024-11-23 17:20:30,951 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51639 2024-11-23 17:20:30,951 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51640 2024-11-23 17:20:30,951 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51641 2024-11-23 17:20:30,951 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51642 2024-11-23 17:20:30,951 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51643 2024-11-23 17:20:30,951 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51644 2024-11-23 17:20:30,952 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51645 2024-11-23 17:20:30,952 - Protocol: Ethernet, Source: d8:bb:c1:3b:29:84, Destination: e2:db:18:27
51646 2024-11-23 17:20:30,952 - Protocol: TCP, Source: 192.168.8.101:62067, Destination: 99.181.79.5:44
51647 2024-11-23 17:20:30,952 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51648 2024-11-23 17:20:30,952 - Protocol: TCP, Source: 99.181.79.5:443, Destination: 192.168.8.101:6206
51649 2024-11-23 17:20:30,953 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51650 2024-11-23 17:20:30,953 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51651 2024-11-23 17:20:30,953 - Protocol: Ethernet, Source: d8:bb:c1:3b:29:84, Destination: e2:db:18:27
51652 2024-11-23 17:20:30,953 - Protocol: TCP, Source: 192.168.8.101:62067, Destination: 99.181.79.5:44
51653 2024-11-23 17:20:30,953 - Protocol: Ethernet, Source: d8:bb:c1:3b:29:84, Destination: e2:db:18:27
51654 2024-11-23 17:20:30,953 - Protocol: TCP, Source: 192.168.8.101:62166, Destination: 99.181.67.74:4
51655 2024-11-23 17:20:30,953 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51656 2024-11-23 17:20:30,953 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51657 2024-11-23 17:20:30,953 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51658 2024-11-23 17:20:30,953 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621
51659 2024-11-23 17:20:30,954 - Protocol: Ethernet, Source: d8:bb:c1:3b:29:84, Destination: e2:db:18:27
51660 2024-11-23 17:20:30,954 - Protocol: TCP, Source: 192.168.8.101:62166, Destination: 99.181.67.74:4
51661 2024-11-23 17:20:30,954 - Protocol: Ethernet, Source: e2:db:18:27:4b:01, Destination: d8:bb:c1:3b
51662 2024-11-23 17:20:30,954 - Protocol: TCP, Source: 99.181.67.74:443, Destination: 192.168.8.101:621

Network Environment:

the capture test was conducted on a windows Operating system, Visual Studio Code; the test would capture packets through: level 2 Ethernet, level 3 IP, level 4 TCP and UDP from the latency graph we can see that we have a left skewer meaning that most of the packet transmission through the network would be fast, from 1ms to 15ms the packets bar chart shows you how many packets have gone through what protocols;

as we can see Ethernet is taken the lead because for our current environment we have used an Ethernet connection instead of WIFI;

and finally the throughput chart shows us throughput of bits per seconds for every protocol; in the terminal we can see all the statistics of the same kind from: throughput per second to network statistic and the final statistic after the termination of the program.