TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

Chapter 1

INTRODUCTION

1 INTRODUCTION

In this chapter we have a short introduction of our system what we are developing, then we have the background of the system with also we have mentioned some of our objectives with this system. In the end, we have the significance of our system.

We study Network administration and computer networks. Through our survey, we have come to know that there is no Internet traffic analyzer, that identifies the blacklisted Ip address which is running in our network. So, we will try to make an internet traffic analyzer that will help the admin to analyze and monitor the traffic of the internet in our networks.

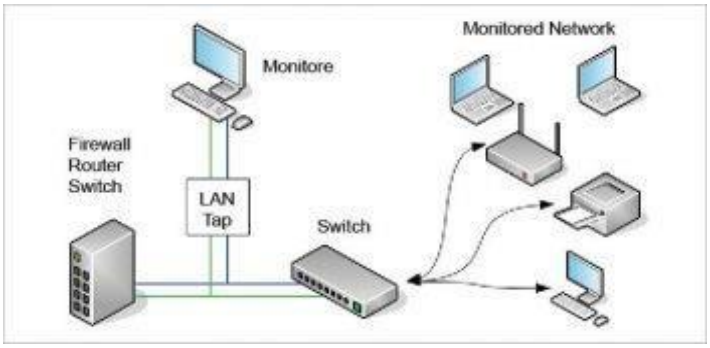

Figure 1: Small Network showing Complete Scenario

1.1 System Introduction

Internet Traffic analyzer is built to offer comprehensive network traffic analysis for all your network elements by automatically collecting and correlating traffic data. Gain insight into network traffic patterns for any network element. ITA is built to collect and analyze flow data from multiple nodes and multiple IP's. ITF identifies the blacklisted IP address from where hacking attempts are performed or illegal activities are performed. The main purpose of internet traffic analyzer is to play an important role in network maintenance, troubleshooting, and network security as well. The typical use of a packet analyzer is to analyze network traffic, troubleshoot the network. It can help identify malicious activity, Increase the efficiency of the network by identifying the blacklisted IP. A Network Traffic Analyzer decoded or dissects the data packets of common protocols like TCP, ARP, UDP, SMTP, etc., and displays the captured packets in a

human-readable format. The captured traffic is decoded and further used to detect various types of network attacks.

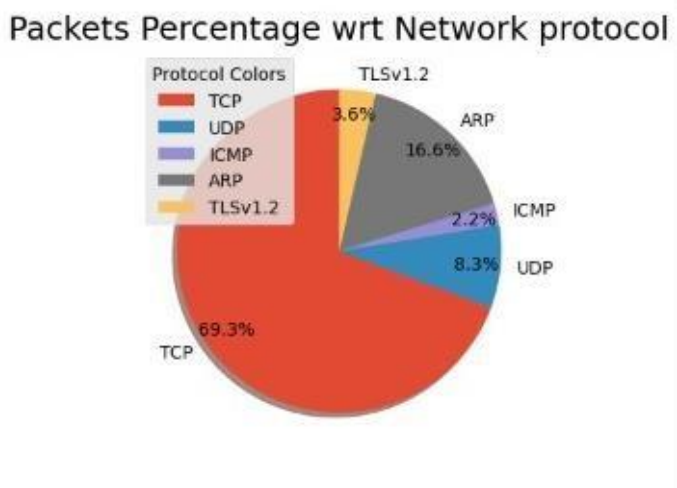

Figure 2: Showing Runtime Network Protocols

1.2 Background of the System

Network traffic analysis is the process of collecting and examining network data to understand and improve the performance of your network. Network traffic analysis can allow you to identify bottlenecks in your network causing slowdowns or may soon impact the quality of service for end-users.

Network traffic analysis is often focused on leveraging flow data for insights into bandwidth usage across your network. Networks are designed with a limited amount of bandwidth. When an array of applications, endpoints, and users are using this bandwidth, performance issues can arise.

With network traffic analysis, you can identify bandwidth-consuming applications, users, protocols, or IP address groups, also known as “top talkers.” In this way, network traffic analysis can help you avoid overloading your network capacity and ensure the end-user experience is satisfactory. Traffic analysis is an activity to record knowledge from user activities in exploiting the net. This study aims to induce knowledge concerning the results of traffic throughout a graphical type so that it will verify the number of users who access the net and use bandwidth.

Internet traffic analyzer is installed on the gateway machine and traffic captured can be then used for network statistics collection, network debugging, and as far as advanced security monitoring and information collection suites.

In this project our focus is on the blacklisted IPs, to identify them. Objectives of the System.

The main objective is to capture network traffic and inspect it deeply to determine what is happening on the network. The network analyzer decodes or dissects the data packets of common protocols e.g., TCP, ARP, UDP, ICMP, IGMP, POP3, etc. including header and footer. and displays the captured packets in Human-readable format for further analysis.

1.3 Objectives of the System

The theme of the project is to monitor the network and help the network admin to secure its network. The main objectives of the proposed system are:

- Capture Traffic.
- Identify Protocol.
- TTL.
- Source address information.
- Destination address information.
- Graphs.
- Blacklisted IP.
- Save data.

1.4 Significance of the System

Internet Traffic analyzer is important and useful for monitoring network traffic. With the continuous growth of organization intranets, computer network security administrators need to be wary of the numerous traffics that go through their networks and how to handle them. Without network traffic monitoring and analysis, an organization's cybersecurity solution will not be complete.

Network traffic monitoring or network traffic analysis is a security analytical tool used by computer network security administrators to detect issues that can affect functionality, accessibility, and network traffic security. Therefore, it is a network security technique for

checking the network traffic of internet-connected devices, the type of data the devices are retrieving, and the bandwidth level each device is consuming.

Furthermore, network security admins and other certified network defenders use a network security program for carrying out network traffic monitoring tasks. By joining network security training and certifications, organizations can swiftly troubleshoot and work out network security threats whenever they arise.

Monitoring network traffic helps to solve the following

- Identifying applications or protocols that are running on the network.
- Monitoring of client to server network traffic
- Identifying bandwidth hogs down to a user or device level
- Troubleshooting of the network and application performance issues

Internet traffic analyzer will capture the traffic and then show a graph where the packet is coming and going based on their source and destination IPs. You can identify the blacklisted IPs and see another main task for monitoring.

Chapter 2

REQUIREMENT SPECIFICATIONS

2 REQUIREMENT SPECIFICATIONS

In this chapter, we have mentioned the scope of our product and also a brief description of our product having product perspective, functionality, users, and characteristics and at the end, we have discussed the operating environment of the system. Then we have detailed information about the specific requirements of the system. We have also mentioned the behavior and interface requirements of the system and at the end, we have detailed non-functional requirements.

Internet Traffic Analysis is a process of capturing network traffic and inspecting it closely to determine what is happening on the network. The network analyzer decodes or dissects the data packets of common protocols like TCP, ARP, UDP, etc., and displays the captured packets in Human-readable format.

A traffic analyzer is installed on the gateway machine and traffic captured can be then used for network statistics collection, network debugging, and as far as advanced security monitoring and information collection suites.

In this project windows-based application has been written in Python language to capture network traffic. The graphical interface has been developed using the Tkinter library. The GUI provides an easy interface to view live network traffic as well as save store it to file for further use. For capturing traffic, I can use the socket module.

Based on the captured traffic, the analyzer generates Capture and Protocol-based statistics. It can calculate the no of packets captured, start and end time of capture, total bytes capture, byte rate. The protocol statistics display the number of TCP, UDP, ICMP, and ARP packets as well as the count of their sub-categories. Also, it can generate the list of Blacklisted IP's traveling in the network.

2.1 Product Scope

In this project, we will analyze the traffic of a network but our main focus is on the blocking of blacklisted IPs which is an attack vector for attackers. These IPs are present on google which can be changed on daily basis, so these IPs will be captured from google and newly blacklisted IPs will be captured.

2.2 Product Description

2.2.1 Product Perspective

In this project, we are going to develop an Internet Traffic Analyzer which is a desktop application and can sniff passively the network traffic.

This project will be divided into two parts. In the first part, it will capture the packet and made a graph based on their source and destination IPs. In the second part, it will identify the blacklisted IPs. We use python for coding purposes. The graphical interface will be done using the Tkinter library and for capturing packets, we will use APIs or TCPdump, Wireshark, and Libpcap.

2.2.2 Product Functionality

- To build software through which users can capture packets from the network.
- Packets including UDP or TCP.
- Identify protocols e.g., HTTP, SMTP, TCP, UDP, POP3, ICMP, IGMP etc.
- Forwarding of packets based on source and destination IPs.
- Identifying and blocking blacklisted IPs by comparing them to source and destination IPs.

2.2.3 User and Characteristics

Internet traffic Analyzer associates with enough easy interface that can permit a user to easily navigate and investigate the traffic of a network.

The use of this application involves the following steps.

There will be different options for the user e.g., creating a new file, capture, go, edit, etc. When the user will click capture then it will start capturing packets and when the user will click go the result it will go to the specific packet.

It will talk about the source and destination IPs of the packet.

It will show that either the packet is TCP or UDP, and it will also tell if the packet is HTTP, SMTP, TCP, UDP, POP3, etc.

It will also highlight the blacklisted IPs and will show them on the screen and will block them too.

2.2.4 Operating Environment

This software will operate in Windows environments.

We use Python for the creation of this software. PyCharm is the framework for the creation of an Internet Traffic analyzer.

This software will be work in a graphical user interface which is quite easy for human use.

Figure 3:Showing PyCharm version 3.2

2.3 Specific Requirements

2.3.1 Functional Requirements

Functional Requirement is that requirement which user must fulfill to meet its project scope and objective. This website provides a fair and accurate school system by some features and requirements.

There are several basic needs each traffic analyzer ought to have, both functional and non-functional. The purposeful needs include:

1) Capturing of the packet

2) Show the protocol of the packet

3) Show the source and destination IP of the packet

4) Identify blacklisted IPs

5) Compare blacklisted IPs with source IP (if matched).

2.3.2 Behavioral Requirements

These are the specifications of user interactions with internet traffic analyzer which include traffic analysis, internet engineers, researchers, etc. The following are some of the major behavior requirements.

A vital section for recognizing however the web traffic is generated is the study of the users 'claim design. In distinction to the investigation of web traffic, users 'claim designs do not seem to alter over the years.

Some features of active sessions. There were chiefly short sessions, however, some of the sessions lasted the whole activity amount, two weeks, which is due to the reality that some users have pointed to point file sharing applications running perpetually.

A fascinating behavior, if we have a tendency to take into account the quality of videos, is found within the length of the sessions. Videos with a medium quality have longer session times.

2.3.3 External Interface Requirements

2.3.3.1 User Interface

The login screen is:

In login screen has two options one is to log in as a senior admin and the other is skip, if the user belongs to network administration then they will log in by using an Email address and password. A login panel is created for securing network admin work. And the local user will skip this login page. If the user enters a wrong password or email then a dialogue box appears and the user sees a message you enter the wrong email or password.

Registration screen is:

In the Registration, screen the user registers itself in an application, by adding his Email address, password, and name, then click on the register user button. The admin user sees a message in the dialogue box, User is added successfully. Then the login screen is open and the admin user can log in to the application easily.

The main screen is:

When the user successfully login into the application then the user sees the option to select interface, interface is an option through which the user connects the end device with the internet or in the network. In an application, I have three different kinds of interfaces Ethernet interface, Wi-Fi, and local area connection. On the main user see other options such as file, edit, view, capture, analyses, and help option or button.

Capture screen is:

When the user selects the interface then the capture screen is open and on the capture screen, the user clicks on the capture button to start capturing the traffic of the internet. Users see capture packets and following information about packets such as source address, destination address, protocol, length, and packet number. When the user selects any packet then the user sees details of the packet such as source address, destination address, protocol, length, and packet number, sum, TTL, offset, off, DF, MK, HL, RF, sport, Sport, size of, version and information into the packet.

Graphic and Analyze screen is:

When the user clicks on Analyze then the user sees all the information in the form of graphs. Graphs show run time virtualizations of capture traffic. In graphs, we add three main components, such as Packet percentage concerning network protocol, packet count concerning network protocol, and the packet length.

Save file is:

When the user completes its activity and wants to save the file then simply click on the file option and click to save the file in the local drive. The capture data or traffic is saved in the form of an excel file.

2.4 Non-functional Requirements

241 Performance Requirements

There's a scope of execution to having this product established at your lodging, usually based mostly around streamlining your life as a supervisor or employees half and fast varied procedures. They include:

1) No demand for the front workspace employees to method reservations once guests will embrace their booking subtleties through the frameworks everything happens consequently and your employees do not have to worry.
2) With guest's tributary their subtleties there is less chance of Associate in Nursing inappropriate info being entered. On the off probability that one thing seems bad, you will have a record to demonstrate it wasn't your flaw.
3) A huge live of visitant info is caught by these frameworks, allowing you to enhance each showcasing and visitant administration
4) Better administration and following of compensating guests for or her steadfastness.

2.4.2 Safety and Security Requirements

Internet traffic analyzer required safety and security measures for some reasons due to which the data to be monitored is correct and accurate. The following are some of the safety and security requirements.
Administer, troubleshoot, and manage hardware, software, or services for user environments. Evaluate problems and monitor networks to make sure it is available for further analysis; identify the blacklisted IP's.

2.4.3 Software Quality Attributes

The following are the software quality attributes of the project.

Bandwidth Monitoring:

Examine which users and what applications are using maximum bandwidth, and list down for casual particulars.

Network Traffic Analysis:

View trends in network traffic, and determine top applications and peak usage times. Use a combination of ports and protocols to define unlimited applications, and recognize this traffic exclusively in traffic reports. You can also map applications to IP addresses.
Define departments based on IP addresses, and identify bandwidth use and application use for each department. And also identify the blacklisted IPs for further investigation. Categorize devices, organize them into logical groups, and monitor traffic reports exclusively for groups.

Accounting:

Improve resource utilization accounting with real-time bandwidth and network usage statistics.

Monitor network traffic between two specific sites, which are created based on the IP address or IP network. This feature helps you understand the network traffic behavior between any two user-defined sites.

Accessibility:

The framework will be realistic all through the conventional structure in activity hours

Rightness:

The degree to that program fulfills details, satisfies client crucial

Productivity:

To what extent less assortment of assets and time are expected to accomplish a chose task through the framework.

Respectability:

Anyway, the framework would insecure the information inside the framework and how it keeps away from the data misfortunes. denotative honesty in data tables and interfaces

Versatility:

The structure of the executives' System will run in any Microsoft Windows and humanoid conditions.

Unwavering Quality:

Specify the elements expected to determine the ideal irresponsibleness of the product bundle at the time of conveyance. mean sun-oriented time among disappointments and mean the sun-powered chance to recuperation

Reusability:

What's the adaptability to utilize the possible pieces of the software in elective frameworks still.

Testability:

The effort required to check to affirm proceeds as assumed

Ease of Use:

Anyway, an individual is taken the benefits of the software and the ease of use.

Heartiness:

The strength of the framework to deal with the software works precisely and keep up the information while not looking too abrupt disappointments

Practicality:

What style, cryptography norms ought to be clung to rejections made

Chapter 3

DESIGN SPECIFICATION

3 DESIGN SPECIFICATIONS

In this chapter, we have a brief discussion with the help of clear diagrams about the design specifications of our system. We have a short introduction first then we have a detailed diagrammatical structure including composite viewpoint, logical viewpoint, information viewpoint, interaction viewpoint, state dynamics viewpoint and at last, we have algorithm viewpoint.

3.1 Introduction

Design Specification includes the complete diagrammatical description of our Product's physical, functional or technical elements, attributes, requirements, or performance, related to or used in our design, manufacture testing, operation, and repair, whether in humans, machine-readable, or another form.

3.2 Compositive Viewpoint

It represents our outlined “complete picture” of the software package we've to make. Configuration of composite views establishes the principles that management the behavior and show of analyst attribute information in Initiate applications. for instance, this includes information that can be examined during the monitoring process i.e., protocols, IPs, and bandwidth, etc.

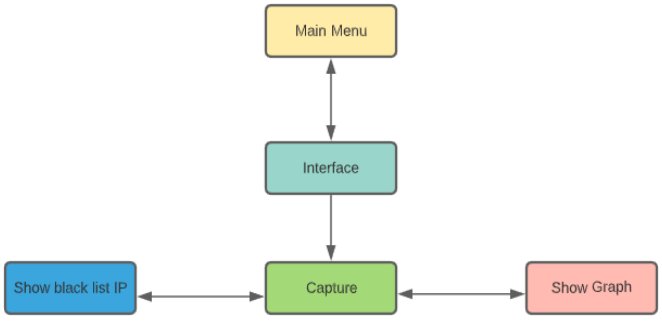

Figure 4: Composite Viewpoint

3.3 Logical Viewpoint

The logical viewpoint is bothered with the practicality that the software provides to end-users. It uses the UML part diagram to explain system parts. the subsequent is that the UML diagram of the software.

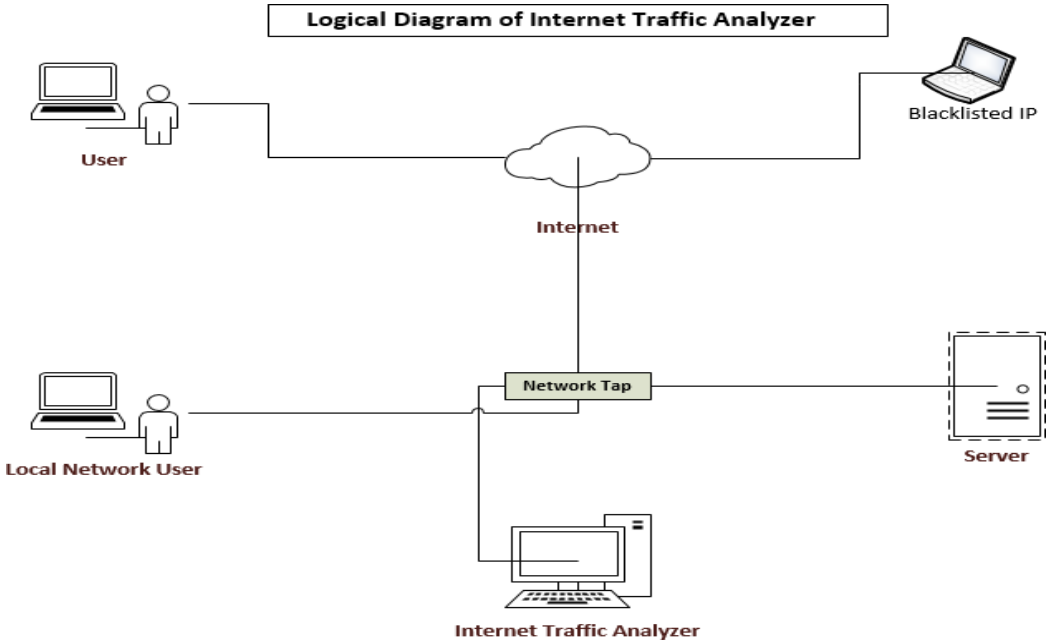

Figure 5: Logical Diagram of complete Scenario

3.4 Class Diagram of Backend

The class diagram of the backend system shows the abstract view of classes that are used in the backend these are not all the classes but some which are major and important.

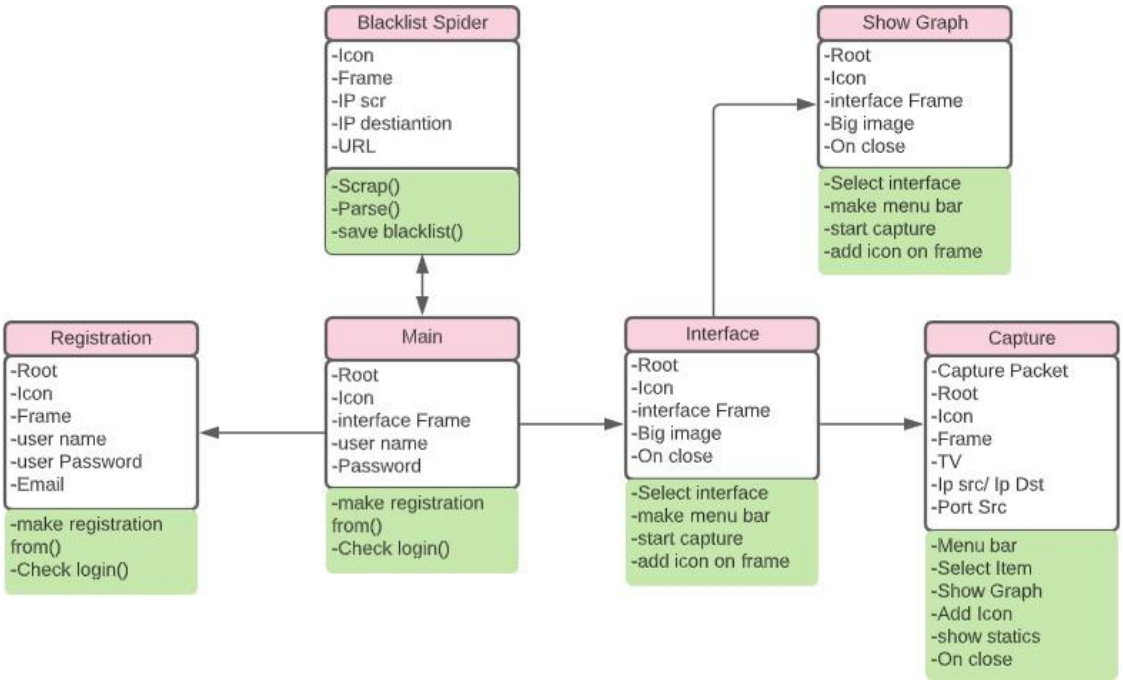

Figure 6: Class Diagram of Backend

3.5 Interaction Viewpoint

3.5.1 Database Design

We are using SQL light database. It is a relation database. SQL light is available in python.

Figure 7: Database Design

3.5.2 Entity Relationship Diagram

Database is absolutely an integral part of software systems. To fully utilize ER Diagram in database engineering guarantees you to produce high-quality database design to use in database creation, management, and maintenance. An ER model also provides a means for communication.

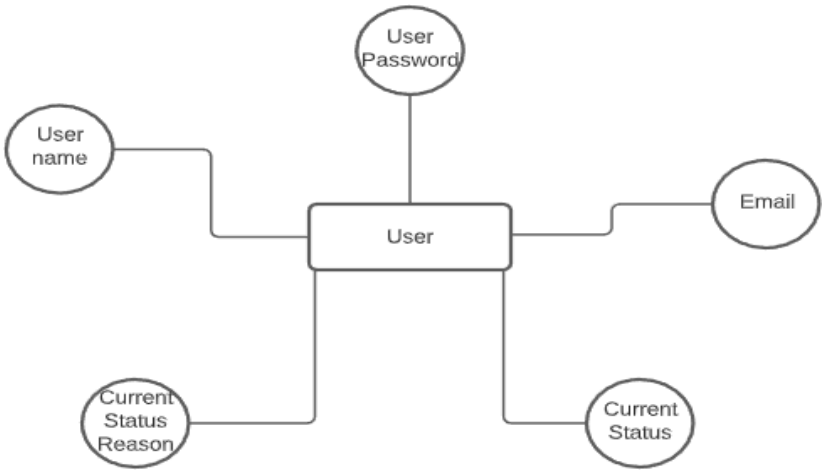

Figure 8: Entity Relation Diagram

3.5.3 Sequence diagram of a system

Interactive software is characterized by vital amounts of interaction between humans and the software. Many users have using Macintosh or Windows computer operating systems, which are prime examples of graphical interactive systems. This software is operating in the graphical user interface.

In interactive View we use sequence diagram shows how the object is interacting and arranged in a time sequence. In the below diagram, have Login, Registration, Interface, Capture, Show Graph and Blacklist entities.

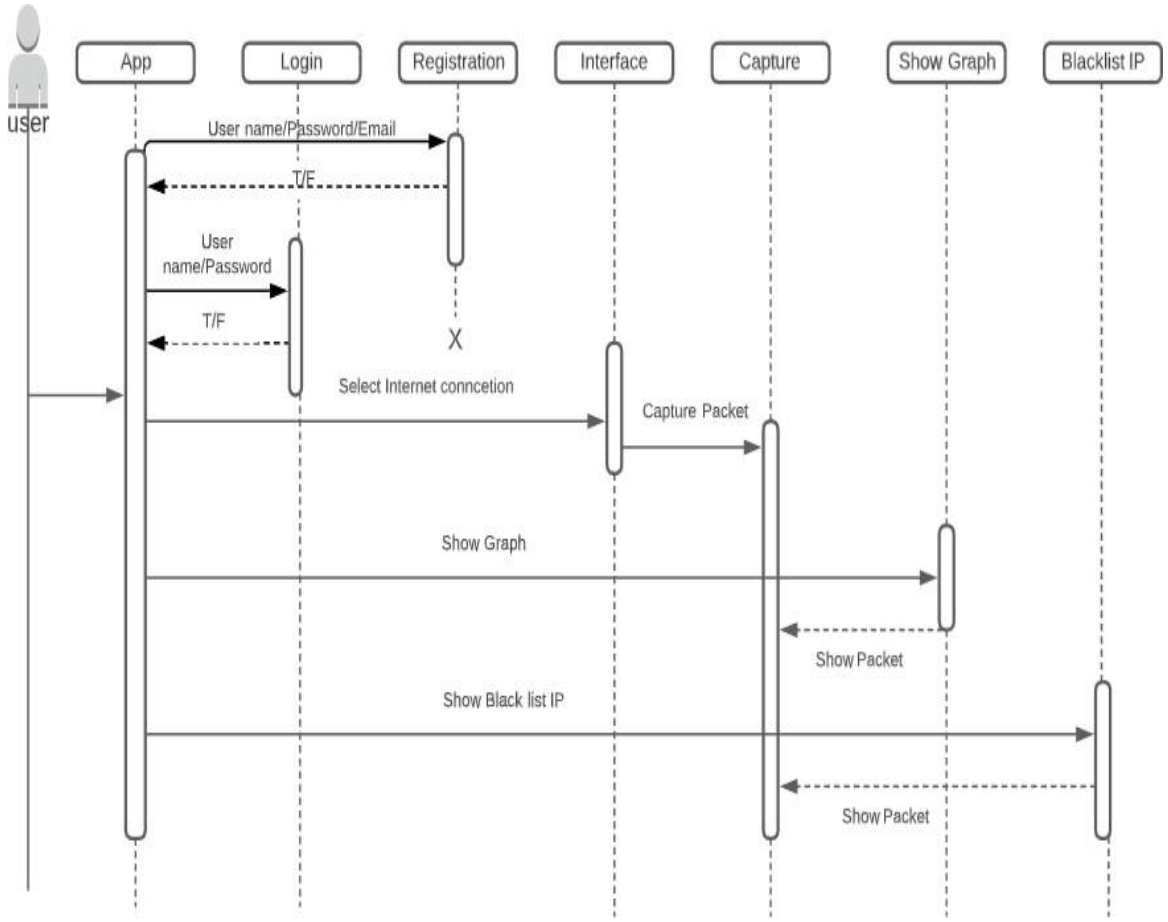

Figure 9: Sequence Diagram

Chapter 4

DEVELOPMENT AND TOOLS

4 DEVELOPMENT AND TOOLS

In this chapter, we briefly discussed our system development team members and the tools which we are used for developing this system, and at the end, we have a conclusion with our future work extensions.

We selected the python language for the creation of this project and the tool we selected is PyCharm. We learned how to capture the packet at first since it was the first move and applied it afterward. We used the lib-cap library to catch the packet for the first few attempts. We had to filter the protocols after that and then show them in the form of graphs.

4.1 Introduction

We have used different tools and techniques to develop this system. User friendly is the priority of the system. Anyone new in the system will easily understand what the system has. The system provides a uniform look and feels between all the interfaces. GUI is simple and understandable. For the development of this project, we selected the python language and the tool we selected is PyCharm. At first, we learned how to capture the packet because that was the first step and then implemented it. The first few attempts were failures then we used the libcap library to capture the packet. After that, we had to filter the protocols and then show them in the form of graphs. We also made a non-functional feature by making the login form, registration form, and data saved in the CSV file. Then we blocked the blacklisted IPs.

4.2 Development Plan

This project is developed by a team of two members.

1. Abdul Hannaan Salik
2. Shahid Mehmood

The workload was distributed among both members equally.

Table 1: Development plan

Task Names	May	June	July	Aug	Sept	Oct	Nov	Dec
Project Approval								
Preparation								
Meeting								
Capturing Packet								
Backend								
Testing								
Documentation								

4.3 Development Tools

4.3.1 Tools

PyCharm (community edition)

4.3.2 Language

Python 3

4.3.3 Packages and Libraries

1. Tkinter
2. pcap-ct
3. libcap
4. dpkt
5. matplotlib
6. pandas
7. Pillow
8. Scrapy

4.4 Conclusion and Future Work/Extensions

To conclude, basically this project was to capture the packets and then analyze them by sniffing the packet. It gives data about the packet but it is in encrypted form. Many other projects capture packets but they are not open source. But this will be open source and will be on GitHub and anyone can download it and can make changes to it in the future. The most unique thing our project does is to identify the blacklisted IPs. The thing we have thought to implement in it is that it will identify which algorithm is used to encrypt the packet. It will be very difficult we will give it a try.

Chapter 5

QUALITY ASSURANCE

5 QUALITY ASSURANCE

5.1 Introduction

Quality Assurance is a procedure to ensure the quality of products or services provided to the users by us. Quality assurance focuses on improving the software development process and making it efficient and effective as per the quality standards defined for software products.
Quality Assurance always ensures that end-users get a functional user interface and the best user experience when using the software.

This chapter, which is mainly based on a test plan, including testing methods and test styles, implemented to ensure the application's reliability and consistency to provide a great and error-free learning experience for the user. Since end-user satisfaction is a first and foremost priority to ensure that a proper test system has been hatched and the results are tabulated in the form of test cases and a requirement traceability matrix has been created to trace each test case against the desired functional requirement, including test case ID against each functional requirement desired by the user.
There might not be anything that happens to switch from creation to production if your solution is new. In certain situations, it is possible to transform the creation environment into a production environment.

5.2 Traceability Matrix

Table 2: Traceability Matrix

Req -ID	Login	Registration	Interface	Capture Traffic	Show Blacklist	Show Graph	Test Case for respective requirement
Req-1		✓					1
Req-2	✓		✓	✓			3
Req-3			✓	✓			2
Req-4				✓	✓		2
Req-5					✓	✓	2
Req-6					✓		1

5.3 Test Plan

A TEST CASE is a set of actions executed to verify a particular feature or functionality of your software application. A Test Case contains test steps, test data, precondition, post condition developed for specific test scenario to verify any requirement. The test case includes specific variables or conditions, using which a testing engineer can compare expected and actual results to determine whether a software product is functioning as per the requirements of the customer. We test our module one by one as they given below.

Table 3: A test case for Registering Members

Test ID	**ABC-1**
Test name	Registering Members
Date of test	10/12/2020
Name of application	Internet Traffic Analyzer
Description	It will tell whether a member is successfully registered or not
Input	Tap on the Register Now button
Expected output	Register successfully
Actual output	Register successfully
Test Role (Actor)	Team Member
Test verified by	Team Member/Supervisor

Table 4: A test case for Capturing Packet through WI-FI

Test ID	**ABC-2**
Test name	Capturing Packet
Date of test	10/12/2020
Name of application	Internet Traffic Analyzer
Description	It will display the packets that are being captured and show the data of the packet
Input	Tap on the Wi-Fi button
Expected output	Captured Packets will be displayed
Actual output	Captured Packets will be displayed
Test Role (Actor)	Team Member
Test verified by	Team Member/Supervisor

Table 5: A test case for Capturing Packet through Ethernet

Test ID	**ABC-3**
Test name	Capturing Packet
Date of test	10/12/2020
Name of application	Internet Traffic Analyzer
Description	It will display the packets that are being captured and show the data of the packet
Input	Tap on the Ethernet button
Expected output	Captured Packets will be displayed
Actual output	Captured Packets will be displayed
Test Role (Actor)	Team Member
Test verified by	Team Member/Supervisor

Table 6: A test case for Blacklisted Ip

Test ID	**ABC-4**
Test name	Blacklisted Ips
Date of test	12/01/2021
Name of application	Internet Traffic Analyzer
Description	It will display the blacklisted IPs packets are detected and show the blacklisted Ips
Input	Tap on the Blacklisted IPs Button
Expected output	Blacklisted IPs displayed
Actual output	Blacklisted IPs displayed
Test Role (Actor)	Team Member
Test verified by	Team Member/Supervisor

Chapter 6

USER MANUAL

6 USER MANUAL

6.1 Introduction

The User Manual contains all essential information for the user to make full use of the software. This manual includes a description of the system functions and capabilities, contingencies and alternate modes of operation, and step-by-step procedures for system access and use.

6.2 Hardware/Software Requirements for the System

Operating System:

- Windows 7
- Windows 8
- Windows 10
- Windows server

Hardware Requirements

- **System:** Multimedia PC, Laptop
- **Processor:** Pentium 4, Dual, core, Xeon
- **Memory (RAM):** 1GB Minimum
- **Display:** SVGA, LCD, LED
- **Modem:** Simple PTCL modem
- **Internet Connection:** Wi-Fi, Ethernet, local area connection

6.3 Installation guide for Application

This is a network application I try to make a user-friendly tool, for traffic analysis. That why first of turn off windows defender, then download an exe file of internet traffic analyzer from google drive. Now double click on .exe file and run-on windows simply then Internet traffic analyzer is installed on the user environment.

6.4 Operating Manual

First of all, the user double clicks on the application icon then the login screen is open and the user has three options, Register, login, and skip now. If the user belongs to the administration group then it's important user will login first and a normal third-party user simply clicks on skip now.

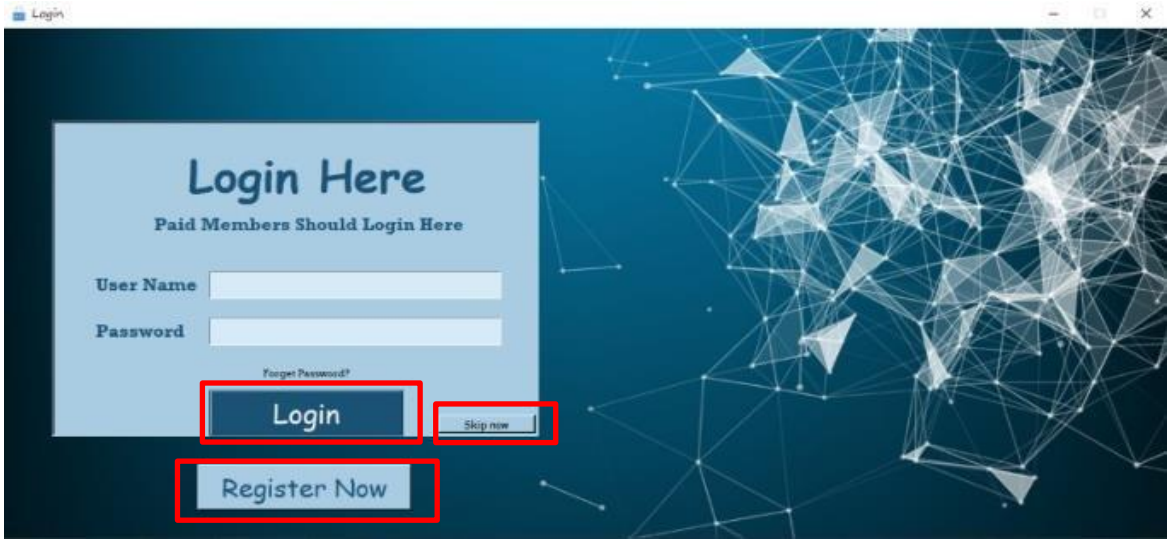

Figure 10: Main Menu

If the user click on the register now button then this foam will open and the user add a user name, email address and password then click on the register

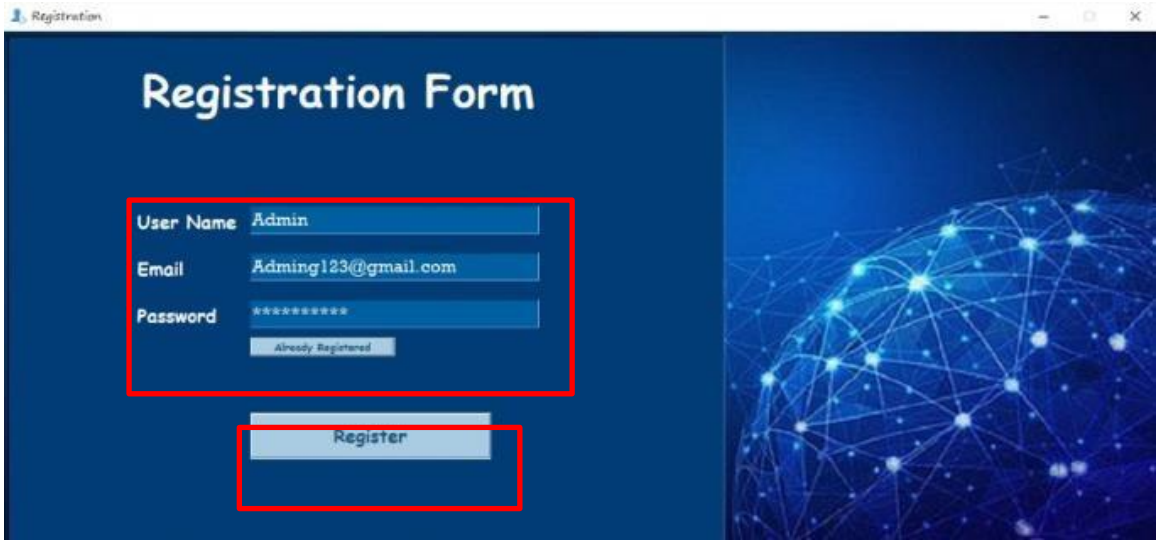

Figure 11: Registration form

Then the user sees a dialogue box successfully register.

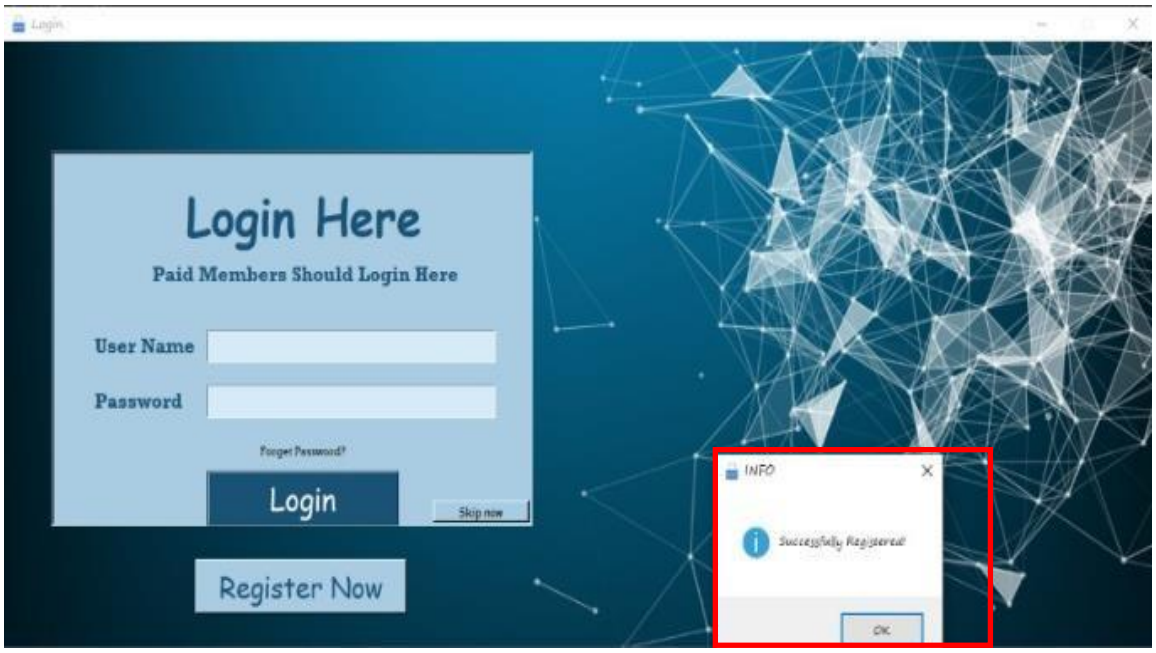

Figure 12: User Register Sucessfully

Now user adds his user name and password and then clicks on login, if the user wants to use the log in option otherwise user can skip now, and then the next window is open.

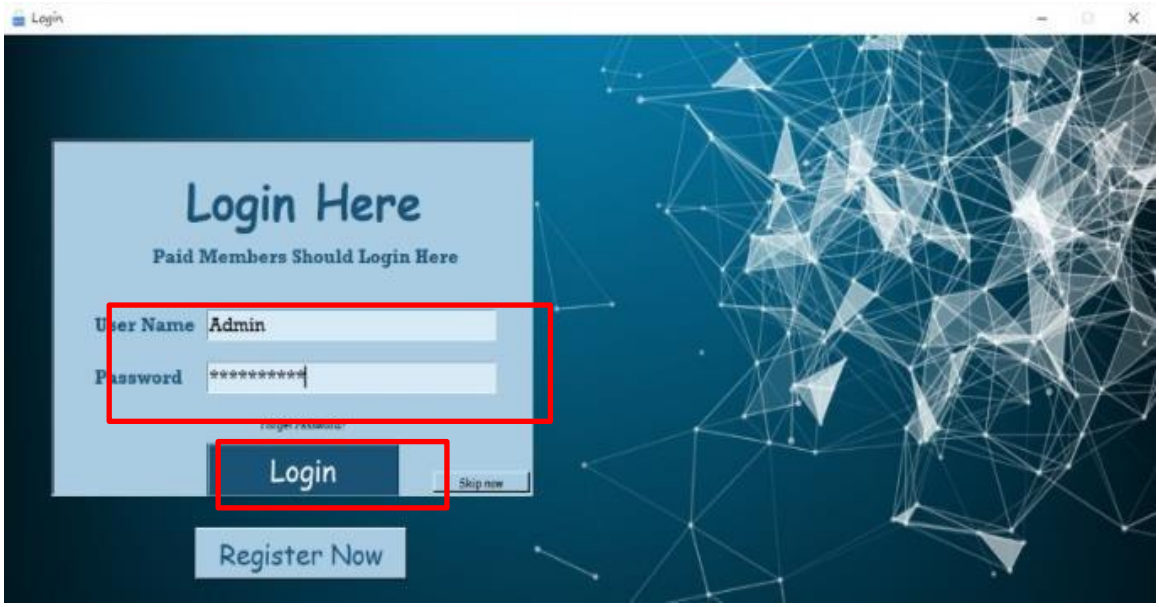

Figure 13: Login Page

Now user login by using ADMIN, Nowhere the user has three options to select his internet connection, one is Ethernet, the second is Wi-Fi and the third is Local Area Connection.

Figure 14: Show Internet Connection

When the user clicks on any interface then only wait for 10 sec and capture traffic is shown on the new window.

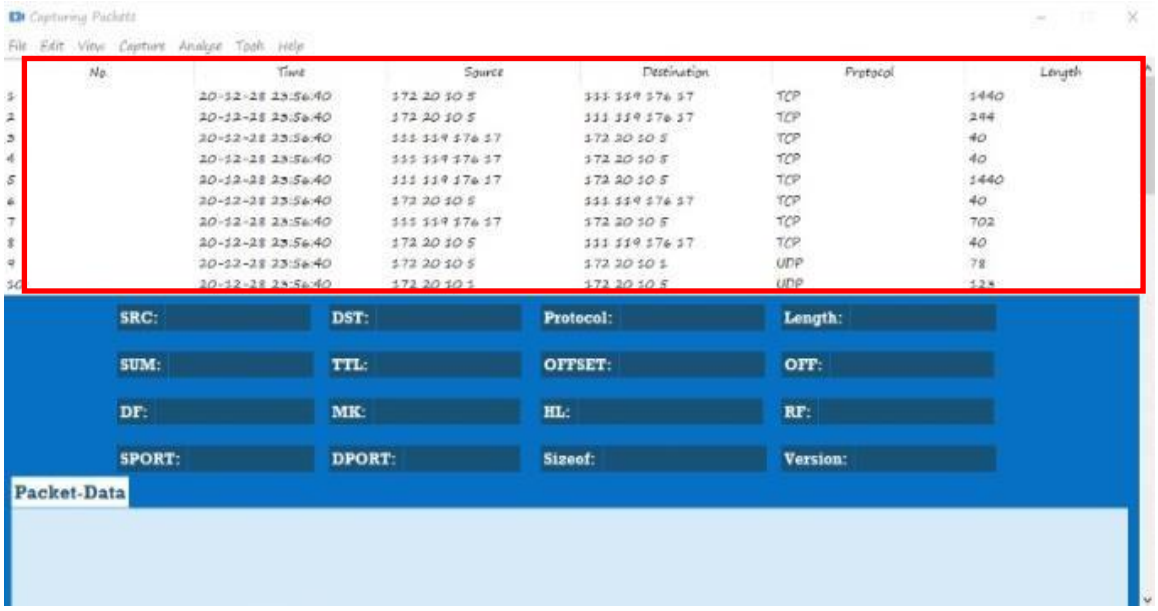

Figure 15: Capture Packet

When the user wants to see any specific packet information then the user simply clicks on any packet and sees packet statics blue boxes.

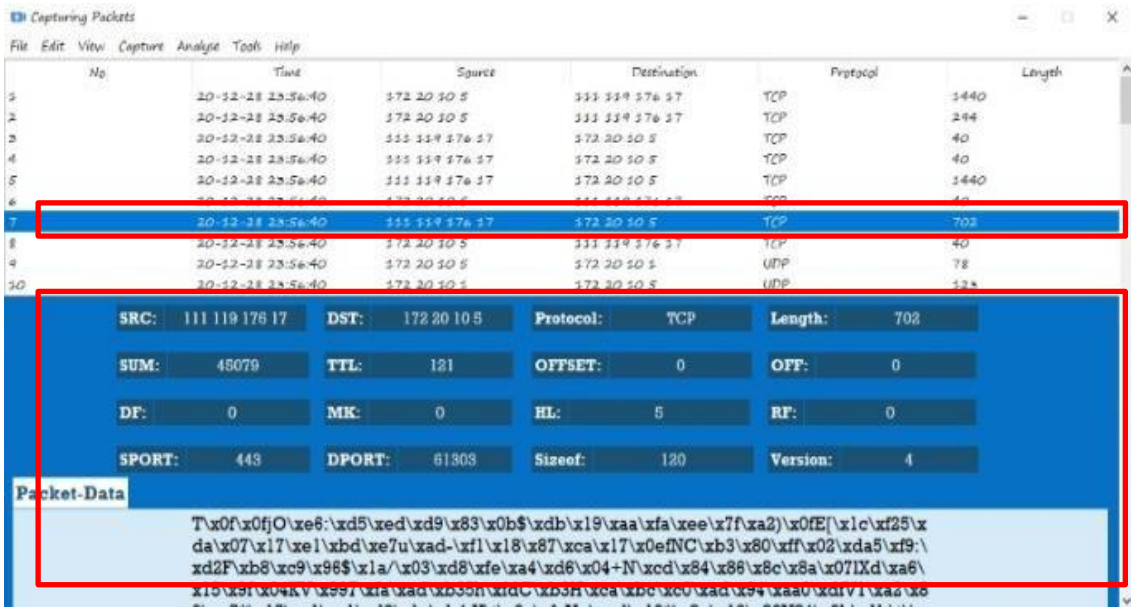

Figure 16: Packet Statics

Now if the user wants to see graphs of capture traffic then the user clicks on to analyze, then click on show stats.

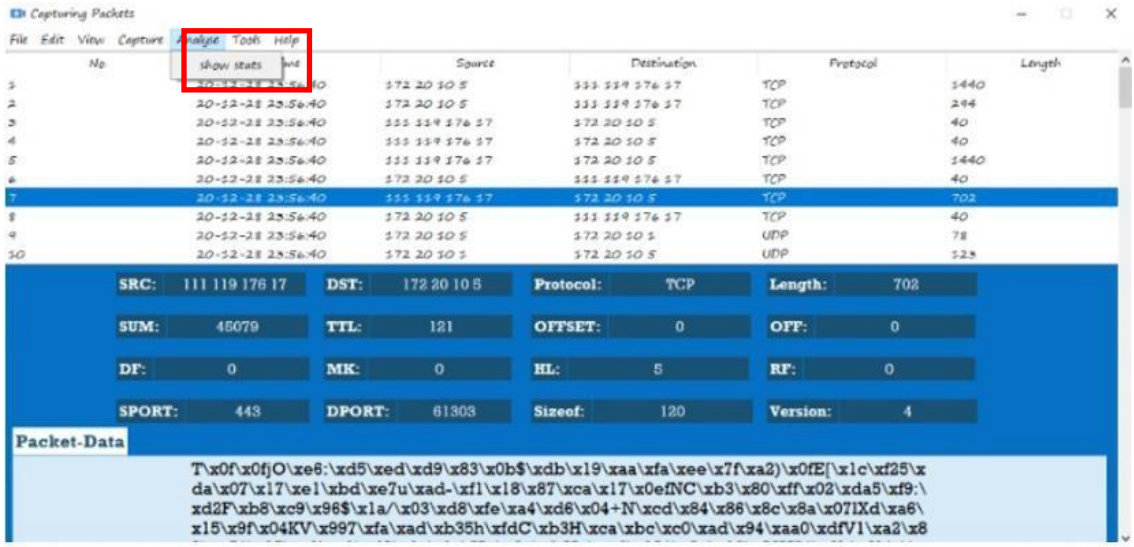

Figure 17: Analyse

Now the user sees three types of graphs.

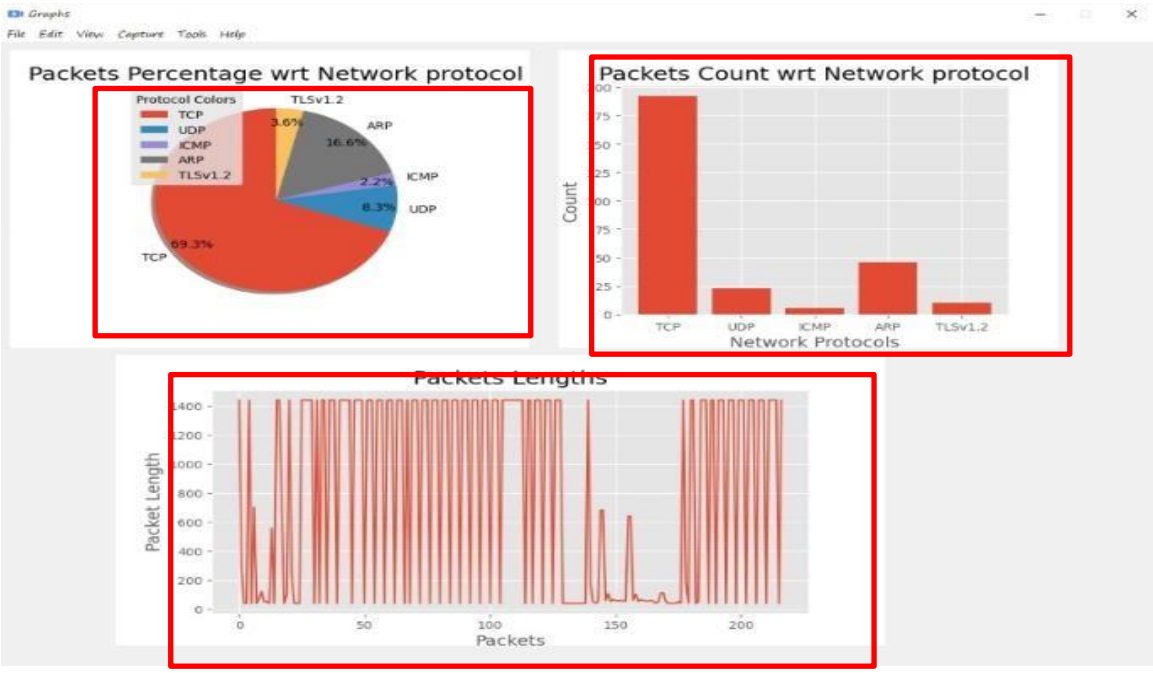

Figure 18: Show Graph

Now if the user wants to back to the capture screen then simply click on Capture and back to capture.

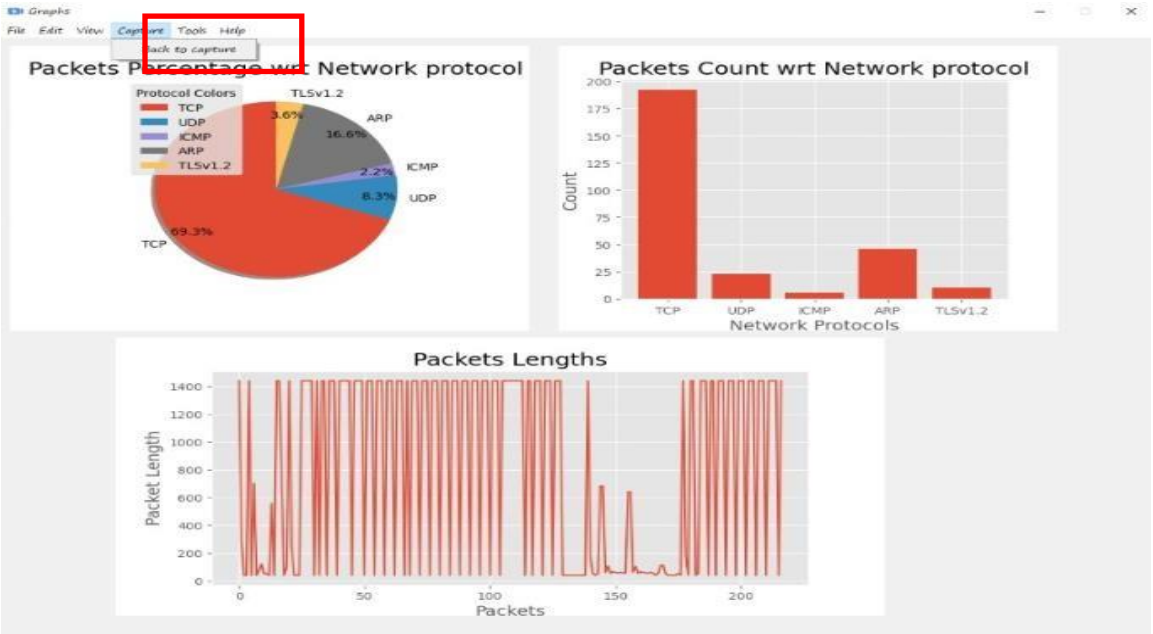

Figure 19: Back to capture

Now is the user wants to save all captured traffic than the user simply clicks on the file button and selects the save option.

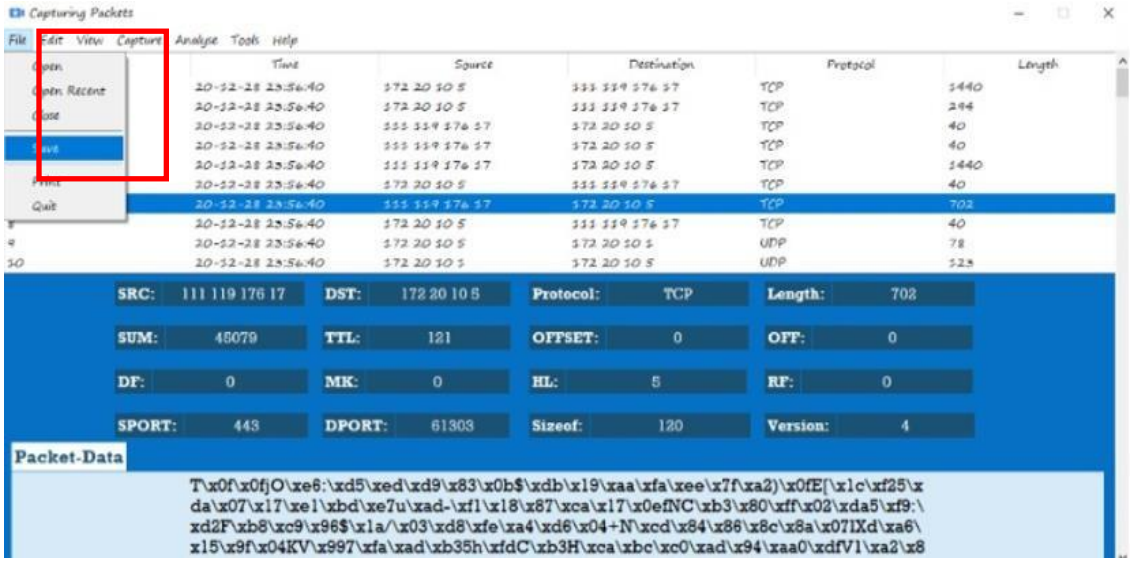

Figure 20: Save file

Then the user sees a confirmation message in the dialogue box successfully saved. The data is saved in an excel file

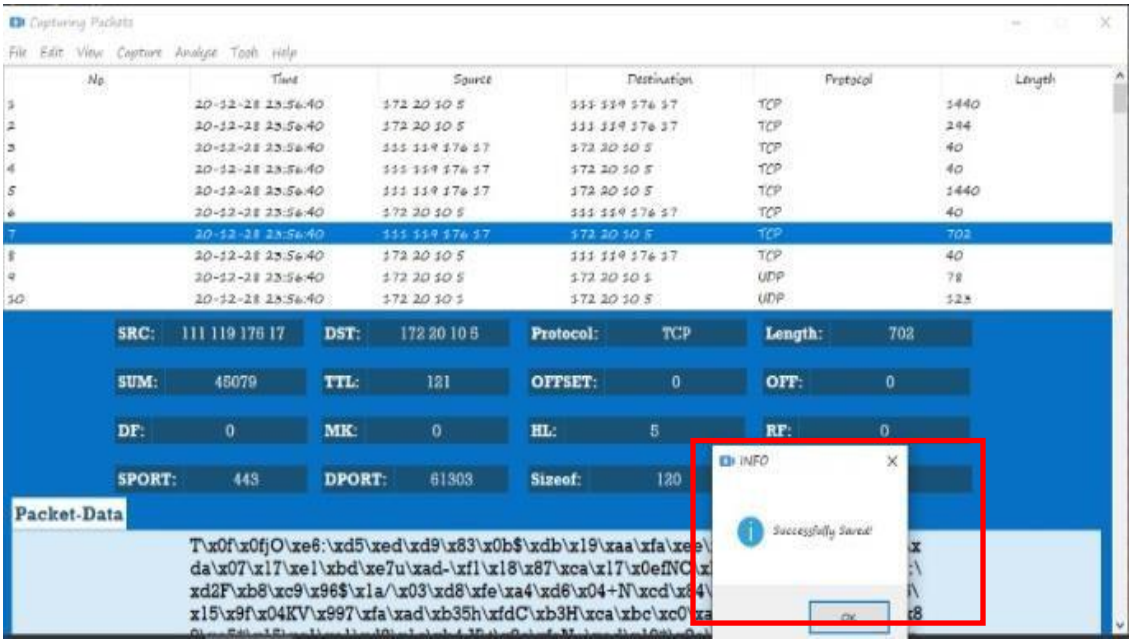

Figure 21: File Successfully save

Now for blacklist Ip address simply click on analyse and then click on Show black list IPs

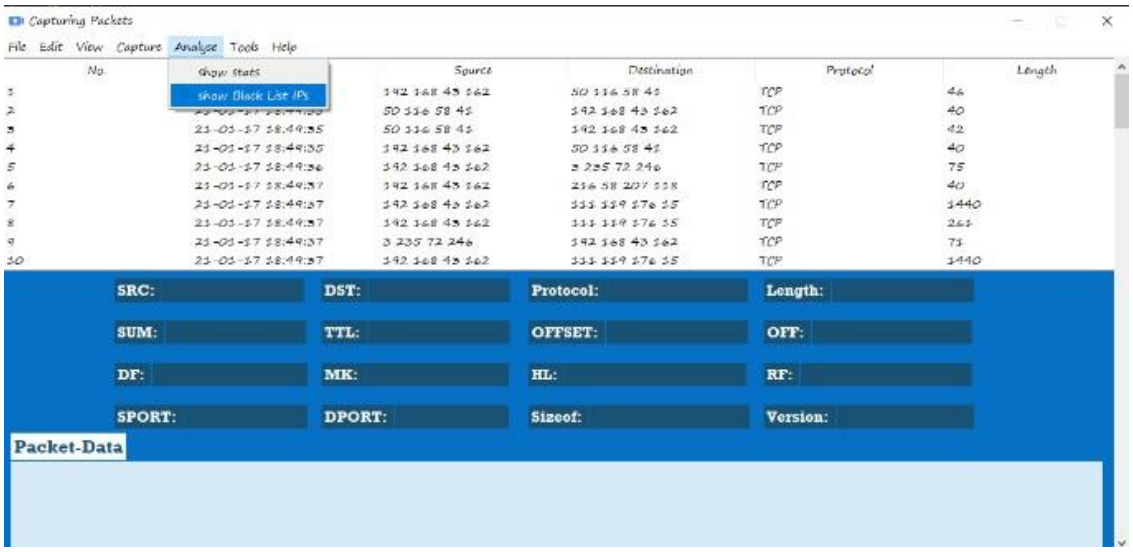

Figure 22: Analyse for Black list IPs

When user click on Show black list ip then user see a diaglouge box in which user see black list Ips if in user network has any blacklist IP.

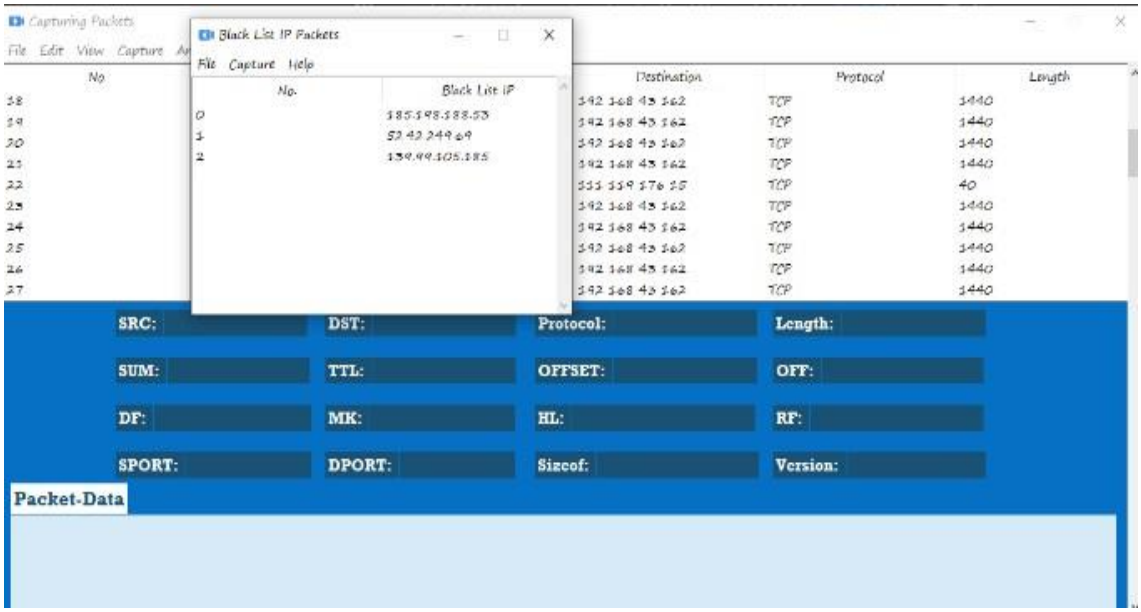

Figure 23: Show black list IP

If user wants to save blacklist Ips then user simply click on File and then click on save.

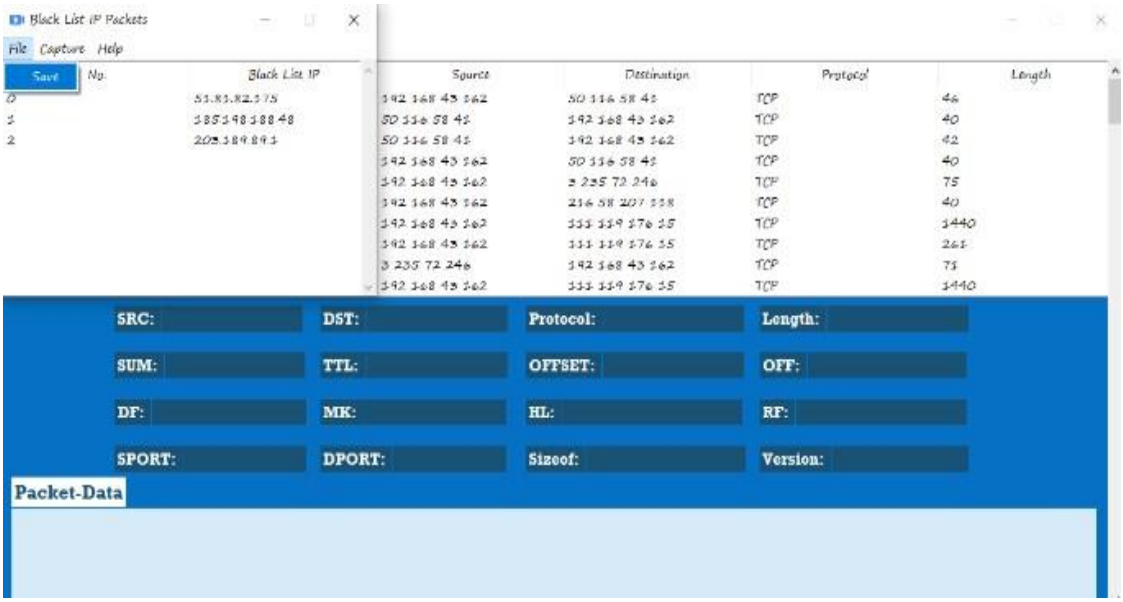

Figure 24: Blacklist IP Successfully save