LOVELY PROFESSIONAL UNIVERSITY

SECTION: KE023

Name- Saurabh SinghVerma

Registration No.- 11916283

ROLL NO: 31

SUBJECT: OPEN-SOURCE TECHNOLOGIES (INT-301)
GITHUB LINK:

QUESTION NUMBER – 14

PROBLEM STATEMENT:

Use any open-source software to view and analyze network traffic (from last 3 months) of the network to which your system is connected. Also generate the report for the same.

INDEX

CHAPTER -1 INTRODUCTION

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

TYPES:

- Disk Forensics: It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- Network Forensics: It is a sub-branch of Computer Forensics that involves monitoring and analyzing computer network traffic.
- Database Forensics: It deals with the study and examination of databases and their related metadata.
- Malware Forensics: It deals with the identification of suspicious code and studying viruses, worms, etc.
- Email Forensics: It deals with emails and their recovery and analysis, including deleted emails, calendars, and contacts.
- Memory Forensics: Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.

- Mobile Phone Forensics: It deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS, etc., and other data present in it. The project that I am doing is under Network Forensics and we will study it now.

Network forensics is the process of analyzing and investigating network traffic to gather information about security incidents or any violations, or events that have occurred on a computer network. This involves capturing data packets and analyzing, logs, and other network traffic to determine the nature of an attack and to what extent an attack happened, and to identify the source of the problem. It can help organizations to understand how a security breach occurred and what data was compromised, and how to prevent similar incidents from happening in the future. It is the main component of computer and network security and is used by law enforcement agencies, businesses, and other organizations to investigate and solve crimes and other security incidents that have happened. Law enforcement will use network forensics to analyze network traffic data harvested from a network suspected of being used in criminal activity or a cyber-attack. Analysts will search for data that points towards human communication, manipulation of files, and the use of certain keywords. Unlike digital forensics, network forensics is more difficult to carry out as data is often transmitted across the network and then lost; in computer forensics data is more often kept in disk or solid-state storage making it easier to obtain.

1.1 OBJECTIVE OF THE PROJECT

The objective of the project is to view and analyze network traffic (from last 3 months) of the network to which your system is connected. The objective of the project is also to gain insight into the network's overall performance and identify any potential security threats or issues.

1.2 DESCRIPTION OF THE PROJECT

This project involves capturing and analyzing network packets that have been transmitted and received by devices on the network. Network traffic analysis is the process of examining network data to gain insights into network performance, usage patterns, security threats, and other important network characteristics. Open-source software tools such as Wireshark, speecy and Usage can be used to capture and analyze network traffic. The process typically involves capturing packets using a network capture tool and storing them in a file format that can be analyzed by the selected network analysis tool. The analysis of network traffic can be used to optimize network performance, identify security threats or attacks, troubleshoot network issues, and improve overall network functionality. By analyzing network traffic, users can gain a better understanding of how their network operates and identify areas for improvement. In this project we used Wireshark to determine the network traffic of the network to which system is connected.

3. SCOPE OF THE PROJECT

The scope of using an open-source software tool is quite broad. Such software can be used to monitor and analyze various aspects of network traffic, including:

1. Security monitoring: - The software can help you detect potential security threats or attacks by monitoring network traffic for suspicious activity.
2. Network utilization: - The software can help you determine how much of the available network bandwidth is being used and by which devices or applications.
3. troubleshooting: - The software can help you identify network issues or errors by analyzing network traffic patterns and identifying areas of congestion or bottlenecks.
4. Performance optimization: - The software can help you optimize network performance by identifying and addressing areas of high network latency or packet loss.

Overall, using network traffic tools is an effective way for network administrators, security professionals, and anyone who wants to understand and optimize the performance of their network.

CHAPTER-2 SYSTEM AND SOFTWARE DESCRIPTION

2.1 TARGET SYSTEM DESCRIPTION:

To capture network traffic of the network, the target system must have a network interface card (NIC) that is capable of capturing network traffic. The target system must have software installed that can capture and analyze network traffic. In addition, the target system must also have sufficient system resources, including CPU, memory, and storage, to handle the capture and analysis of network traffic.

2.2 ASSUMPTIONS AND DEPENDENCIES:

There are several assumptions and dependencies that you need to consider. These include that you need to have access to the network, a compatible network interface, sufficient system resources, proper configuration of the software, knowledge of networking protocols and tools, and the time and expertise to carry out the process.

2.3 FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES:

Functional dependencies are those that relate to the features and capabilities of the open-source software you plan to use. Some of them are Compatibility with the network interface, Support for the network protocols, Ability to filter traffic, Ease of use. Non-functional dependencies are those that relate to the operational and performance requirements of the open-source software. Some non-functional dependencies to consider include System requirements, Performance and scalability, Security, Support and community.

2.4 SOFTWARE DESCRIPTION:

WIRESHARK

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. Packet Capturing: Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. Filtering Information: Wireshark is capable of slicing and dicing all 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.

CHAPTER-3 ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND REPORT:

In this report, we will discuss the network traffic analysis of my system Mac using Wireshark. Wireshark is a network protocol analyzer that allows you to capture and analyze network traffic in real-time. It is a powerful tool that can help you to troubleshoot network problems and monitor network activity. We will go through the steps of using Wireshark to capture and analyze network traffic on your system.

Step 1: Installing and Configuring Wireshark:

The first step I did in using Wireshark is installing it on my system. You can download Wireshark from the official website and install it on your system.

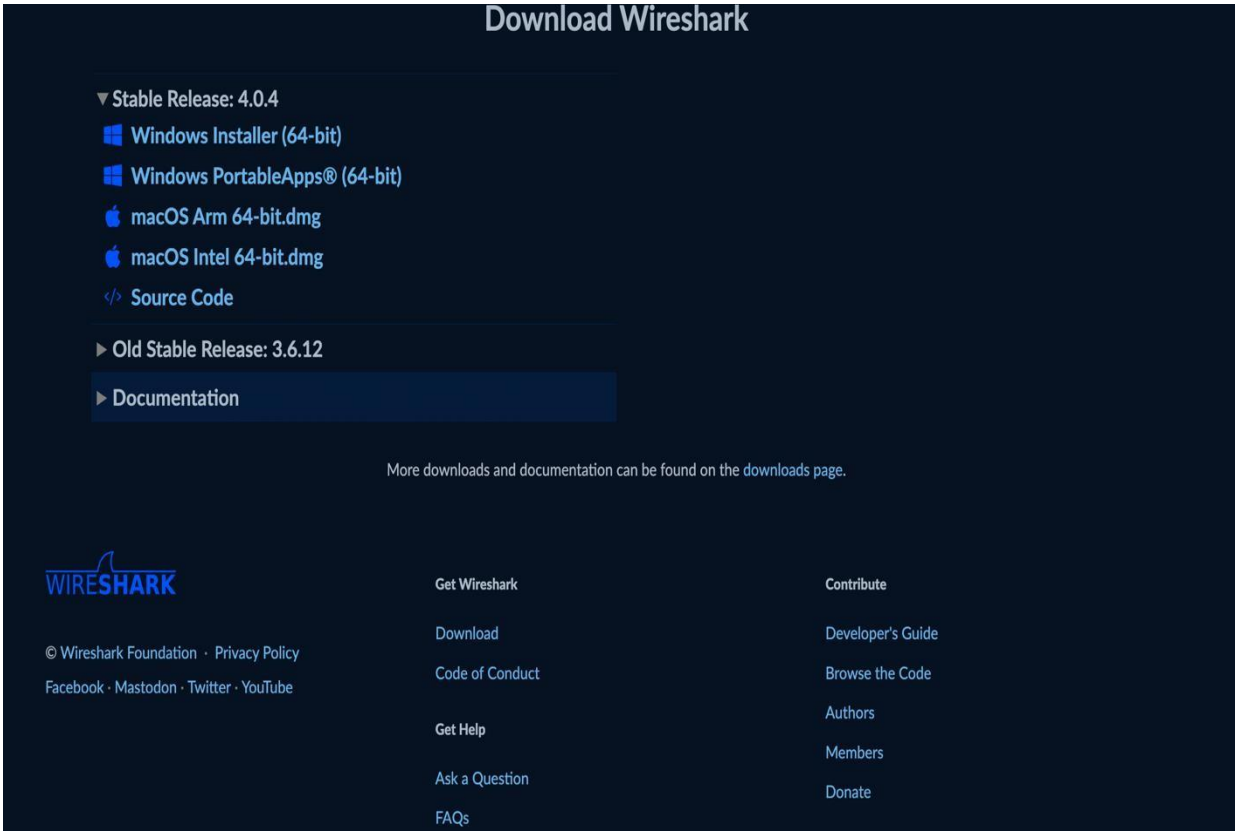

Fig 3.1 different stable releases of software for different operating systems.

Once Wireshark is installed, we need to configure it to capture network traffic on your system. To do this, start Wireshark and select the network interface you want to capture traffic on. You can select the interface from the Capture Options dialog box.

Step 2: Capturing Network Traffic:

Once Wireshark is configured to capture network traffic, you can start capturing traffic by clicking on the Start button in the Capture Options dialog box. Wireshark will start capturing traffic on the selected interface. You can also filter the traffic you want to capture by using capture filters.

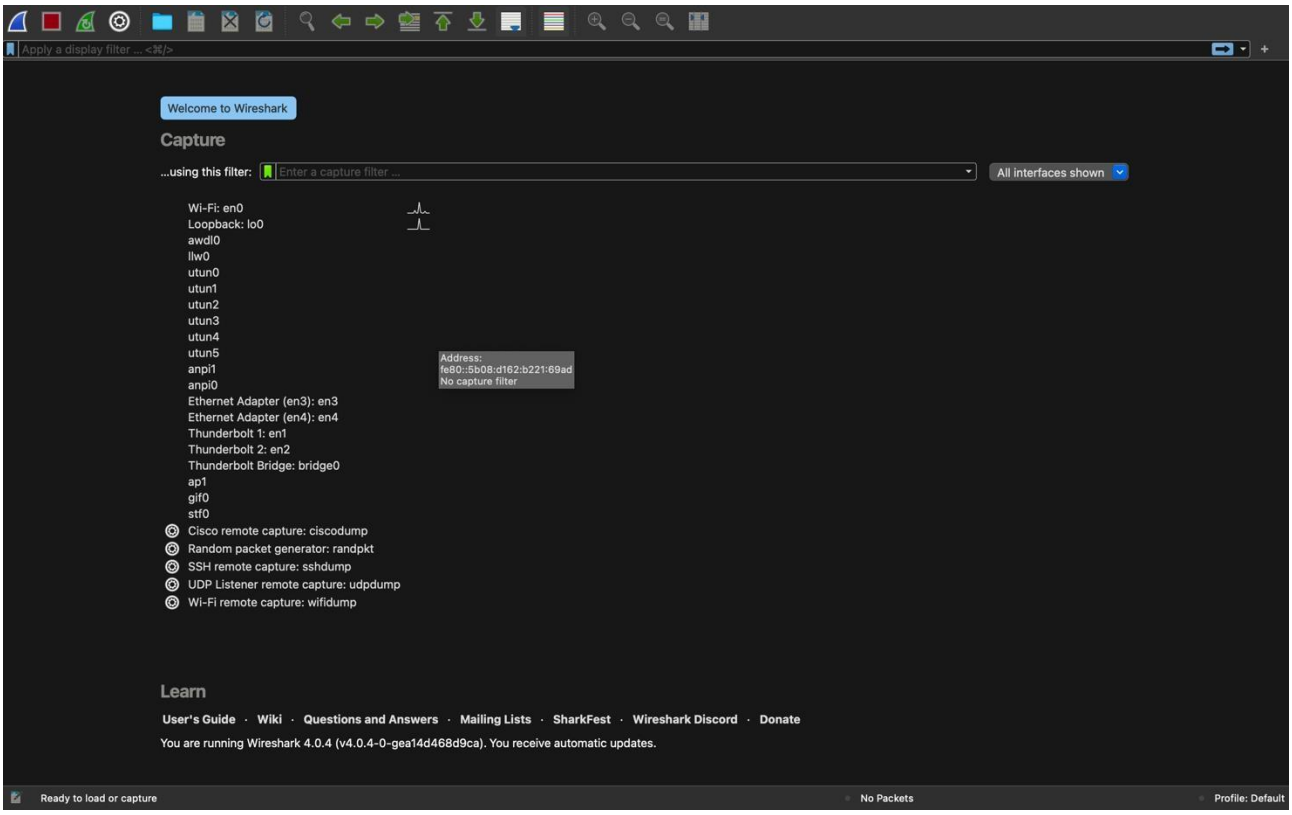

Fig 3.2 Starting interface of Wireshark application displaying all different network options available on system.

For capturing traffic firstly, we need to double click on (Wi-Fi: en0) option to capture traffic of the network that I am connected to. After this we can see a tab displaying network traffic of my Wi-Fi network. It displays the information of time capturing packets, source Ip address, destination Ip address, length of the packet and basic detail of the packet.

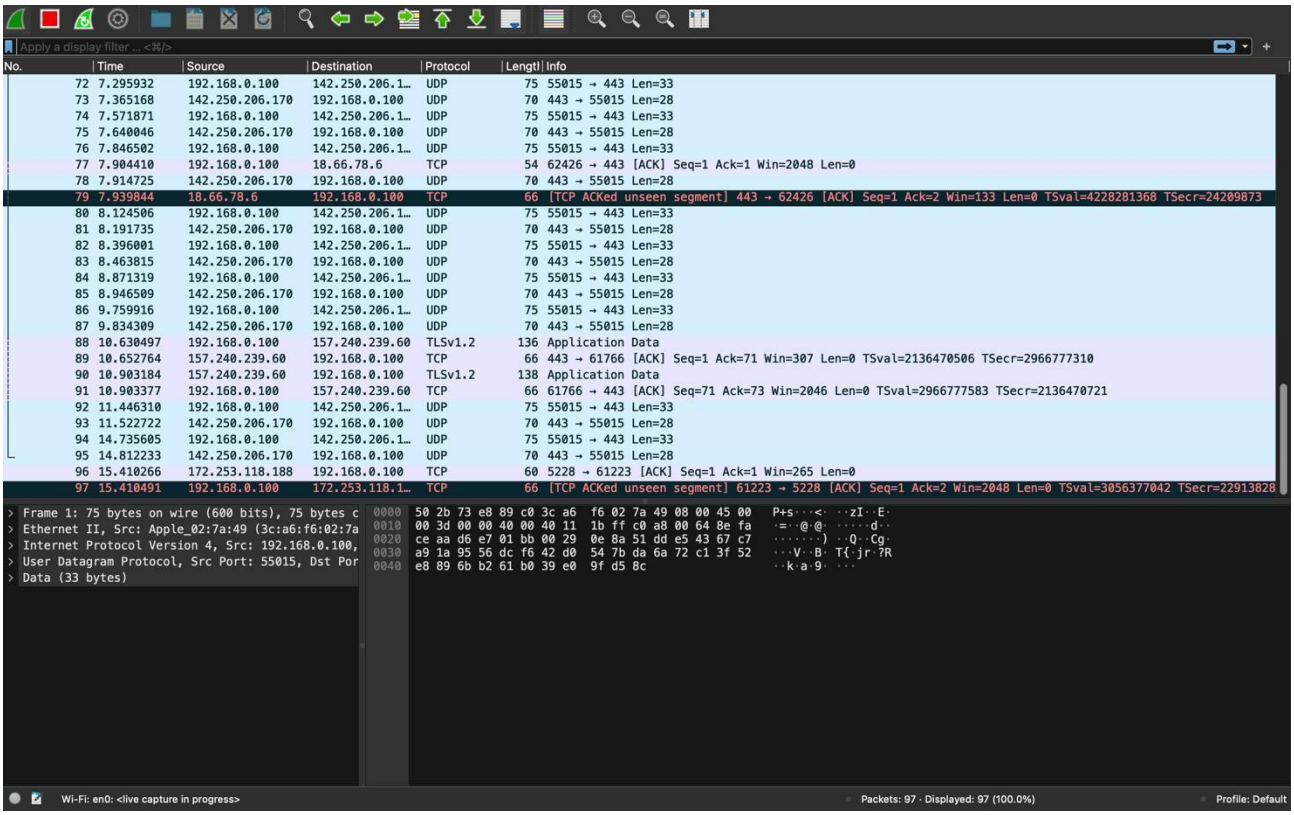

Fig 3.3 Network traffic of the network (Wi-Fi:en0) that we are connected

The information displaying about traffic is of every device that is connected to network and if we want to display the network traffic of our system, we need to go to edit option above in the toolbar and select the option capture and then it displays a tab where we can choose the host system for the network traffic in our system.

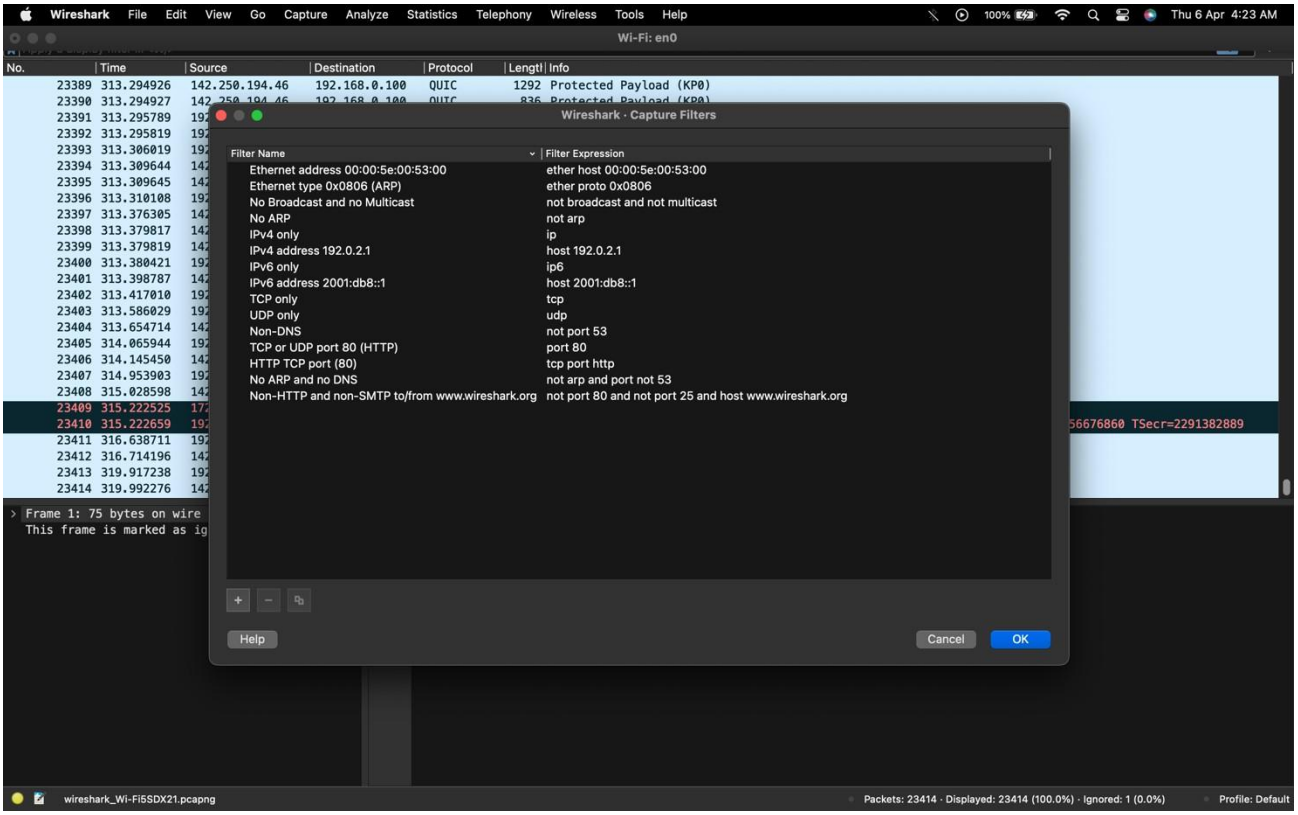

Fig 3.4 Selecting the host system and Filtering the traffic related to our system

After selecting the Host system, we can see the network traffic of our system. After this step we can proceed to analyze the traffic and monitor it.

Step 3: Analyzing Network Traffic:

After capturing network traffic, you can start analyzing it using Wireshark. Wireshark provides a lot of features and tools to analyze network traffic. You can analyze traffic based on protocols, conversations, endpoints, and more. Wireshark provides detailed information about each packet captured, including the source and destination addresses, packet size, protocol used, and more. In Wireshark we can also view the traffic of the other systems. For that we just must go to STATISTICS > I/O GRAPHS > DISPLAY FILTER and we must enter Ip address of the system to get the network traffic of that system.

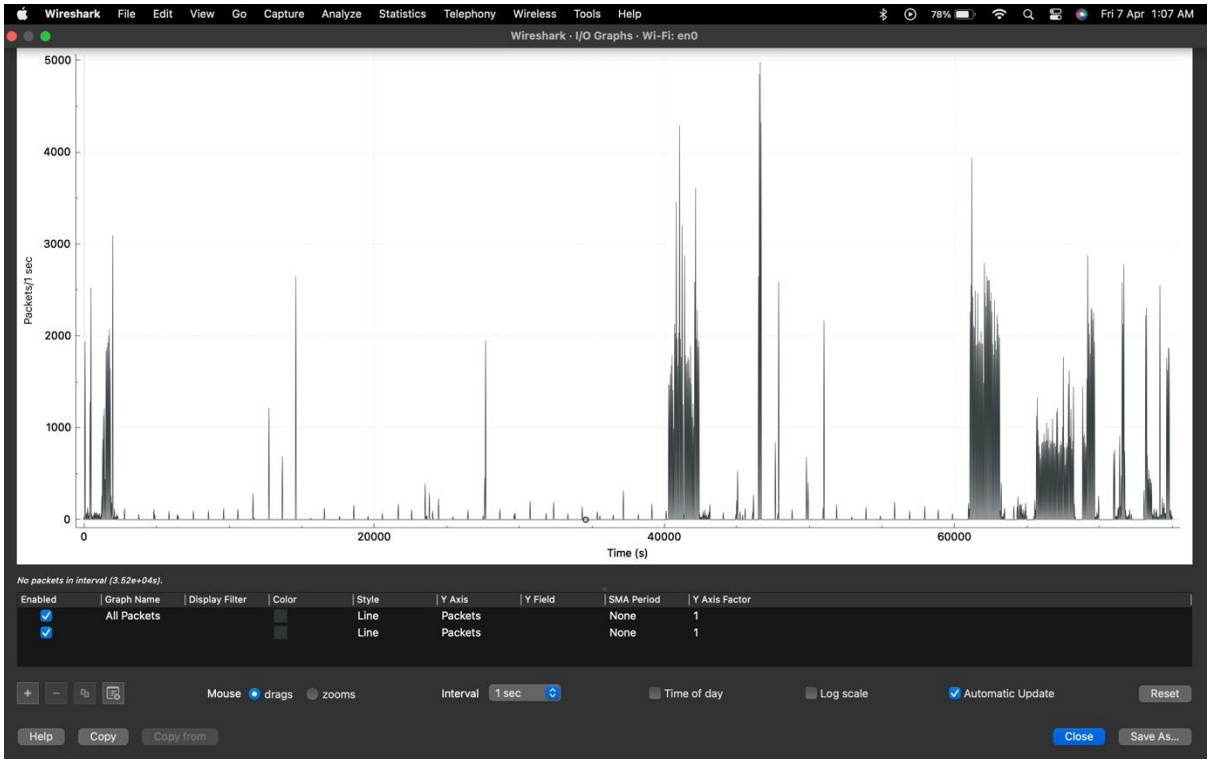

Fig 3.5 I/O Graph of the connected network displaying packets per second that are being captured.

Step 4: Troubleshooting Network Problems:

Wireshark is an excellent tool for troubleshooting network problems. It allows you to capture and analyze network traffic to identify the source of network problems. For example, you can use Wireshark to identify network congestion, packet loss, and other network issues.

CHAPTER-4 CONCLUSION

In conclusion, capturing and analyzing network traffic using open-source software can be useful for network administrators and security professionals. With the right tools and expertise, it is possible to gain insights into network traffic patterns, identify security threats, and optimize network performance. However, it is efficient to consider the assumptions, functional dependencies, and non-functional dependencies when working on such a project. Wireshark is an essential tool for network traffic analysis. It allows you to capture and analyze network traffic in real-time and troubleshoot network problems. In this report, we discussed the steps of using Wireshark to capture and analyze network traffic on your system. I hope this report has provided you with a good understanding of network traffic analysis using Wireshark.

REFERENCES :

1 https://www.techtarget.com/searchsecurity/definition/computer-forensics

2 https://www.geeksforgeeks.org/introduction-of-computer-forensics/

3 https://www.cybrary.it/blog/0p3n/introduction-to-computer-forensics/

4 https://en.wikipedia.org/wiki/Computer_forensics

5 https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

6 https://www.itpro.co.uk/cyber-attacks/31660/what-is-network-forensics