

Name- Arbas Rahaman

Registration No: 11917273

Subject Code – INT 301

Section – KE015

Roll No: 32

Submitted To: Dr. Manjot Kaur

Academic Task 2

# Index

1. Introduction
   1. [Objective of the project 5](#_TOC_250002)
   2. [Description of the project 5](#_TOC_250001)
   3. [Scope of the project 5](#_TOC_250000)
2. System Description
   1. Target system description 6
   2. Assumptions and Dependencies (If applicable) 6-7
3. Analysis Report
   1. Final result of the Microsoft edge 7-10
   2. Final result of the Firefox 10-11
   3. Final result of the Google 11-13
4. Reference/ Bibliography 14
5. Github-link 15

# Chapter 1

### Introduction

#### What is computer forensics?

Computer forensics involves applying investigative and analytical techniques to collect and safeguard evidence from a specific computing device in a manner that is admissible in a legal setting. The aim of computer forensics is to conduct a systematic inquiry and create a well-documented trail of evidence to determine precisely what occurred on the computing device and who should be held accountable for it.

#### Types of computer forensics

There are various types of computer forensic examinations. Each deals with a specific aspect of information technology. Some of the main types include the following:

* 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 the 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 mainly 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.

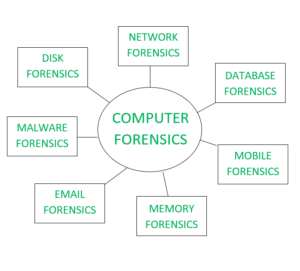


Fig:1 Types of Computer Forensics

**Network Forensics**

Network forensics is a subset of digital forensics that focuses on inspecting network activity and the traffic passing through a network that is believed to be associated with malicious operations, such as a network that is disseminating malware to steal login information or to conduct cyber-attacks analysis. The importance of network forensics has increased in tandem with the expansion of the internet and the rise of cybercrimes, particularly with the proliferation and acceptance of network-based services like the World Wide Web, email, and various other digital communication mediums.

Through the use of network forensics, it is feasible to recover all data, including messages, file transfers, emails, and web browsing history, and reconstruct them to reveal the original transactions. While the payload in the top-layer packet may also end up on the disk, the packets used to transport it are solely recorded in network traffic. Therefore, the network protocol data that encapsulate each communication are often highly valuable.

For identifying the attacks investigators must understand the network protocols and applications such as web protocols, Email protocols, Network protocols, file transfer protocols, etc.

Investigators use network forensics to examine network traffic data gathered from the networks that are involved or suspected of being involved in cyber-crime or any type of cyber-attack. After that, the experts will look for data that points in the direction of any file manipulation, human communication, etc. With the help of network forensics, generally, investigators and cybercrime experts can track down all the communications and establish timelines based on network events logs logged by the NCS.

**Processes Involved in Network Forensics:**

* Identification: In this process, investigators identify and evaluate the incident based on the network pointers.
* Safeguarding: In this process, the investigators preserve and secure the data so that the tempering can be prevented.
* Accumulation: In this step, a detailed report of the crime scene is documented and all the collected digital shreds of evidence are duplicated.
* Observation: In this process, all the visible data is tracked along with the metadata.
* Investigation: In this process, a final conclusion is drawn from the collected shreds of evidence.
* Documentation: In this process, all the shreds of evidence, reports, conclusions are documented and presented in court.

#### Objective of the project

To generate a daily report of internet usage from 9pm-7am in your hostel/home.

#### Description of the project

To collect internet usage data from 9 pm to 7 am using Wireshark, you will need to set up a packet capture filter that captures network traffic during this time frame.

To do this, you can use the time filter option in Wireshark. First, go to the "Capture" menu and select "Capture Filters." In the "Capture Filter" dialog box, select the "Time" option and set the start time to 9:00 PM and the end time to 7:00 AM.

Once the filter is set, you can start the packet capture. Wireshark will capture all network traffic during this time frame, including websites visited, file downloads, and other internet usage activities.

After the capture is complete, you can analyze the captured data in Wireshark. You can apply filters to isolate specific types of traffic, such as HTTP traffic (web browsing), FTP traffic (file transfers), or DNS traffic (domain name lookups). Wireshark also provides a range of statistics and visualization tools that can help you understand the patterns and volume of internet usage during the specified time period.

#### Scope of the project

Analyzing internet usage from 9 pm to 7 am using Wireshark can provide valuable insights into network activity patterns, including web browsing habits, application usage, and other online behaviors. Some of the potential areas of scope for analysis are Protocol Analysis, Traffic Volume, Website Visits, Application Usage, Security Analysis.

Overall, analyzing internet usage from 9 pm to 7 am using Wireshark can provide valuable insights into network activity patterns and user behavior. However, it's important to note that capturing and analyzing network traffic should be done with appropriate permissions and in compliance with applicable laws and regulations.

**Chapter 2**

### System Description

#### Target system description

To generate a daily report of internet usage from 9 pm to 7 am in your hostel or home, the ideal target system would consist of a network device like a router or switch that can capture network traffic. This device should have the capability to run network traffic capture tools like Wireshark, which can capture and analyze the network traffic within the specified time frame.

Along with the network device, the system would also require a computer or server that can run Wireshark and generate reports based on the captured data. The computer or server should have sufficient processing power and storage capacity to handle the volume of data captured during the specified time frame. Additionally, it should be configured to run Wireshark on a daily basis to capture and analyze network traffic.

Other critical considerations for the target system include network security measures to safeguard the system and captured data from unauthorized access. Backup and disaster recovery protocols should also be in place to prevent data loss in the event of hardware or software failures. Finally, the system should be configured to generate reports in an easy-to-read format that provides relevant information on internet usage during the specified time frame.

Other important considerations for the target system might include network security measures to protect the system and the captured data from unauthorized access, as well as backup and disaster recovery procedures to ensure that data is not lost in the event of hardware or software failures. The system should also be configured to generate reports in a format that is easy to read and understand, and that provides relevant information on internet usage during the specified time frame.

#### Assumptions and Dependencies (If applicable)

* The target system has the necessary hardware and software capabilities to capture and analyze network traffic during the specified time frame.
* The target system is connected to the network that is being monitored and has access to all relevant network traffic.
* The target system is configured with appropriate network security measures to ensure the privacy and confidentiality of captured data.
* The target system is dependent on the availability and stability of the network being monitored. Any network disruptions or downtime may affect the accuracy and completeness of the captured data.
* The accuracy of the daily report is dependent on the accuracy and completeness of the captured data. Any missed or incomplete data may affect the accuracy of the report.
* The successful operation of the network traffic capture tool and software is dependent on the compatibility and stability of the target system's hardware and software.

**Chapter 3**

## Analysis Report

#### This is the final result after capturing:

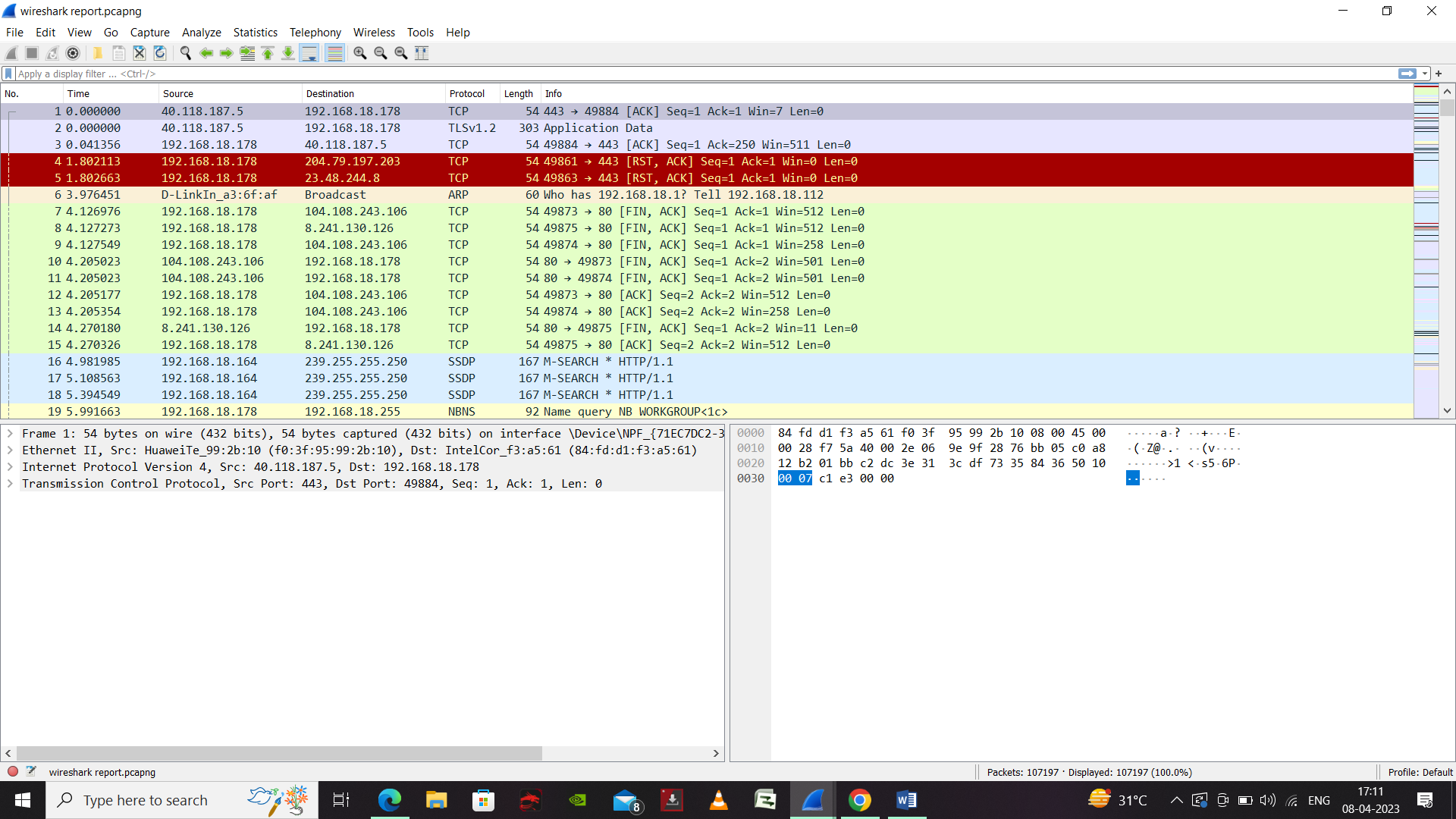
****

Figure.1 Wireshark report

This is the Wireshark Forensic Report after capturing the internet usage which shows different parameters like time, source, destination, protocol, length and info.

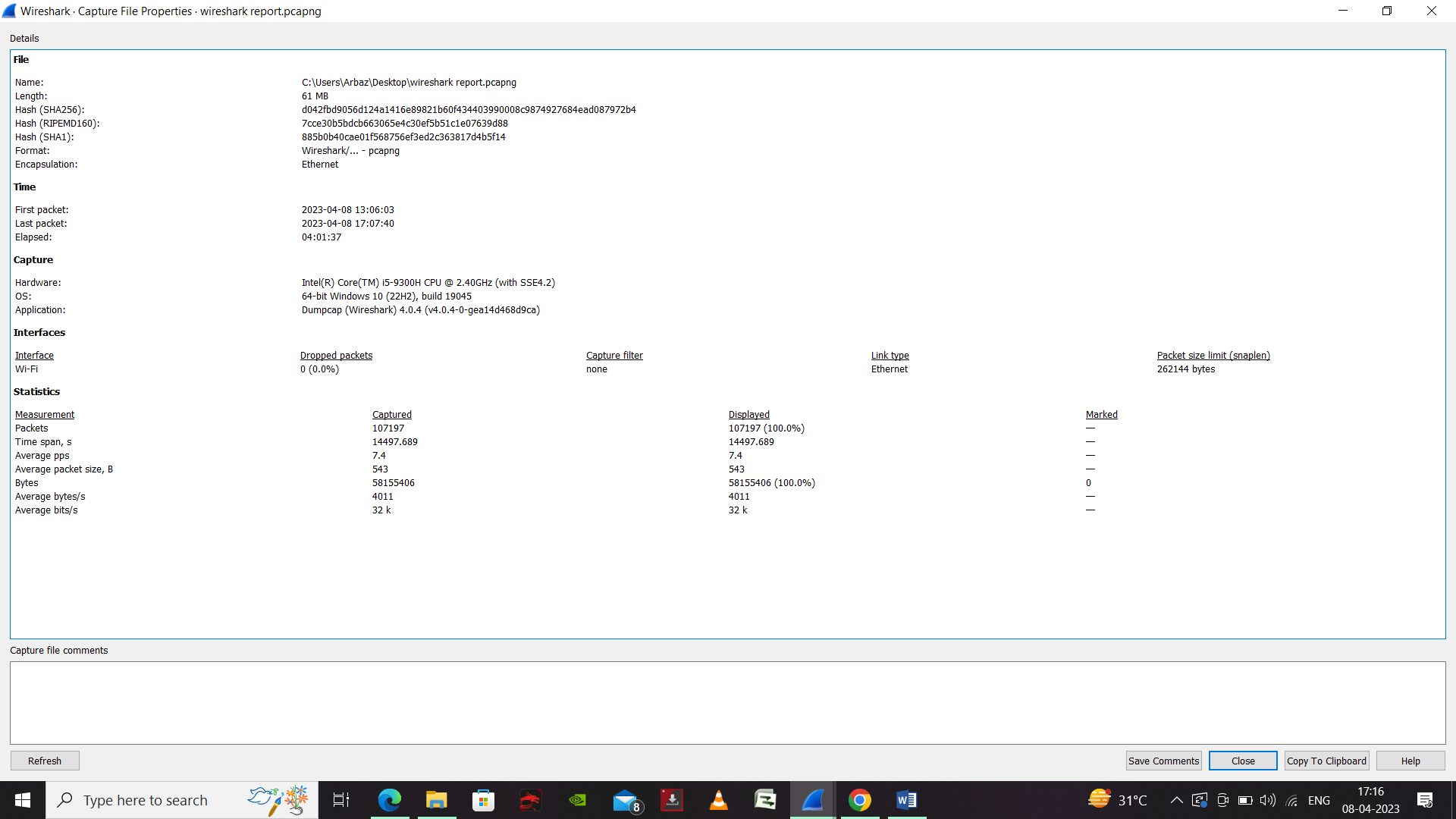


Figure.2 Capture File Properties

In Figure 2 indicates the Capture File Properties in Wireshark provides information about the captured network traffic, such as the capture file format, the timestamp precision, the captured packets' count, and other details.

* File Name: The name of the capture file.
* Capture Interface: The name of the network interface that was used to capture the network traffic.
* Capture Duration: The length of time that the capture file covers.
* Packet Count: The number of packets captured in the file.
* File Size: The size of the capture file in bytes.
* Encapsulation Type: The network protocol used to encapsulate the captured packets, such as Ethernet, IP, or TCP.
* Time Precision: The precision of the timestamps used in the capture file, such as microseconds or nanoseconds.

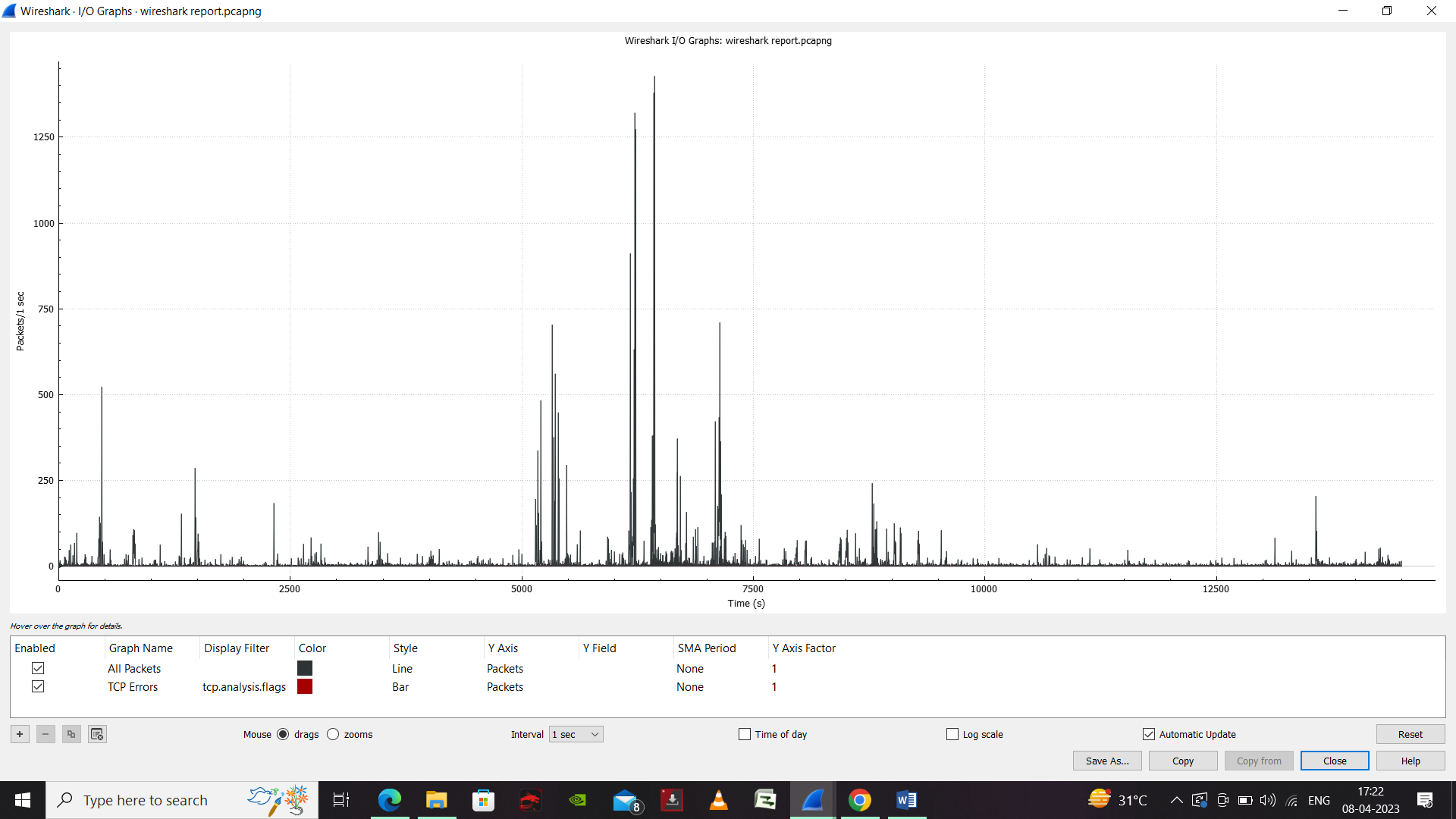


Figure.3 Input Output Graph

The input/output graph in Wireshark is a graphical representation of the traffic flow between hosts in a network capture. It shows the amount of traffic exchanged between hosts over time, which can help you identify the busiest hosts or applications on the network.

By default, the IO Graph shows the amount of traffic exchanged between all hosts in the capture file. You can customize the display by selecting different fields from the "Graph" and "Y-Axis" dropdown menus. For example, you can choose to display the amount of traffic exchanged between specific hosts or using specific protocols.

We can also use the input/output graph in Wireshark, you can get a visual representation of the traffic flow in a network capture and identify patterns or anomalies in the network traffic.

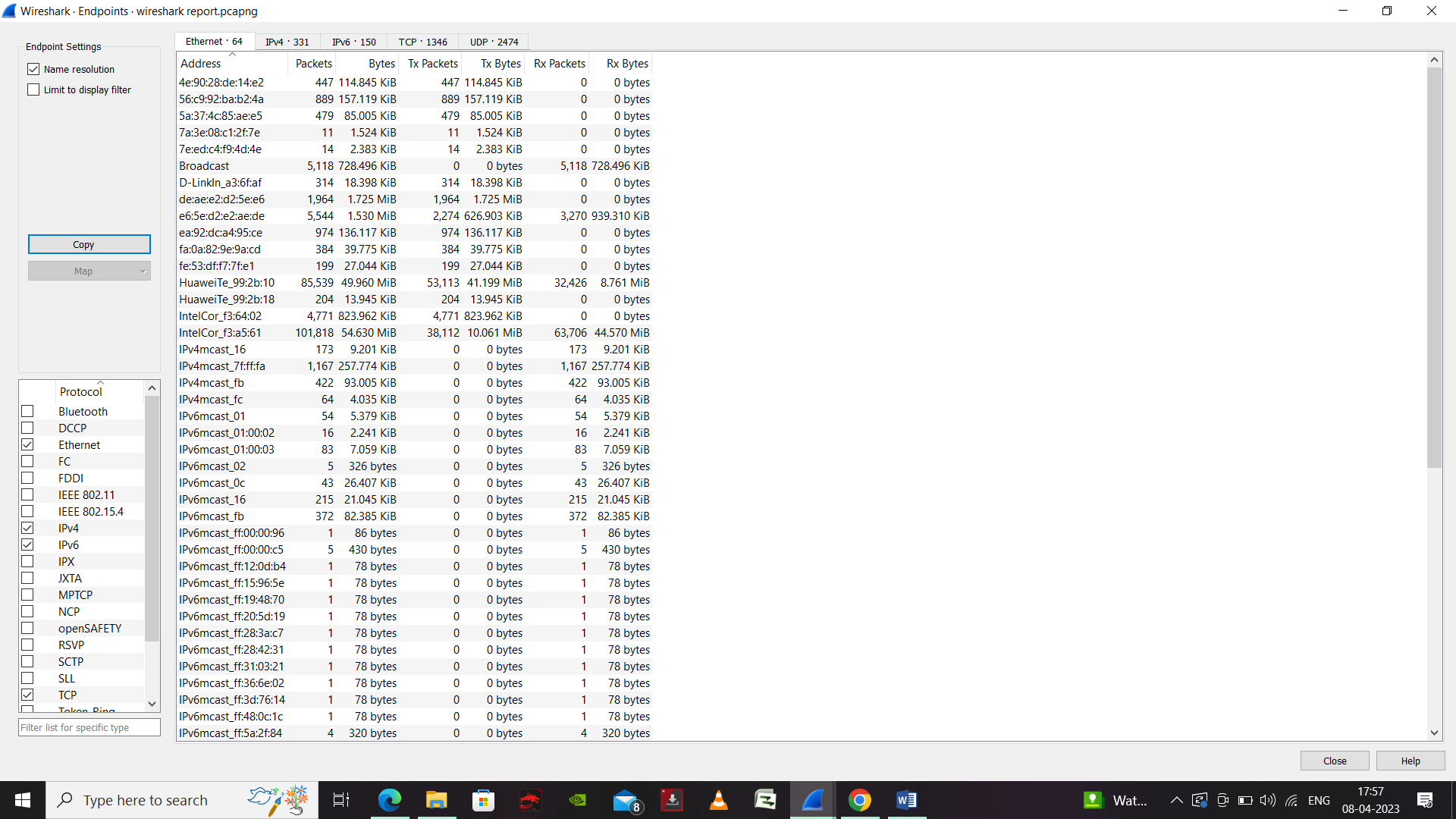


Figure.4 End Point

Endpoints in Wireshark refer to the network devices or hosts that are involved in the captured network traffic. The Endpoints dialog in Wireshark provides a summary of the endpoints involved in the capture and allows you to filter the captured packets based on the endpoints.

By using the Endpoints dialog in Wireshark, you can quickly identify the hosts and devices involved in the captured network traffic and filter the packets based on the endpoints. This can help you analyze the network traffic in more detail and troubleshoot network issues more effectively.

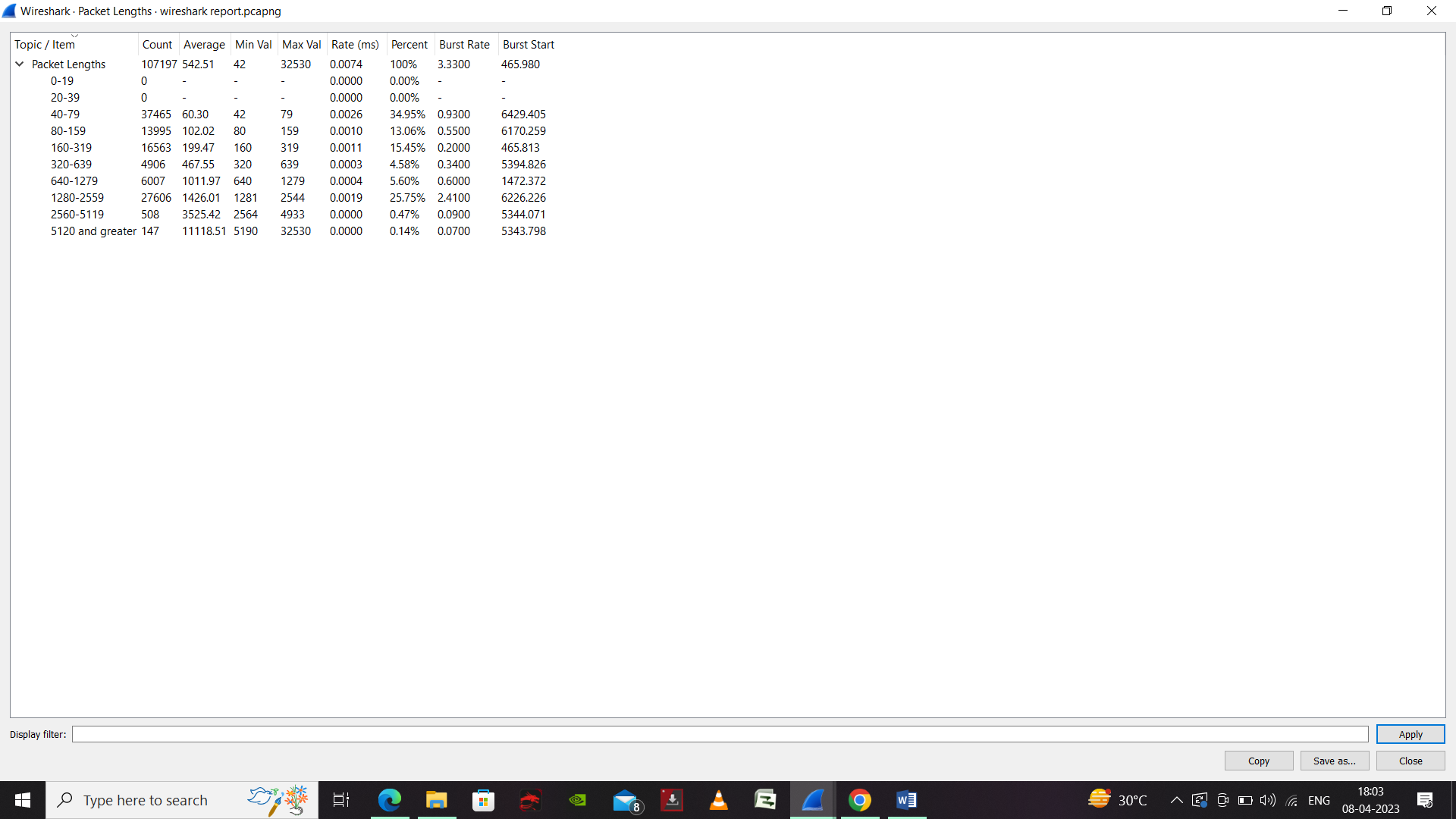


Figure.5 Packet Lengths

The Packets Lengths feature provides a statistical analysis of the size of each packet captured in a network traffic capture. It can help you analyze the traffic patterns and identify any anomalies or errors in the network traffic.

By analyzing the packet length statistics, you can identify patterns or anomalies in the network traffic. For example, you might notice that certain packets are much larger than others, indicating a potential problem with the application or network configuration.

The Packets Lengths feature in Wireshark provides a useful way to analyze the sizes of packets captured in a network traffic capture, which can help you identify issues and troubleshoot network problems.

#### This is the final result of the Protocol Hierarchy:

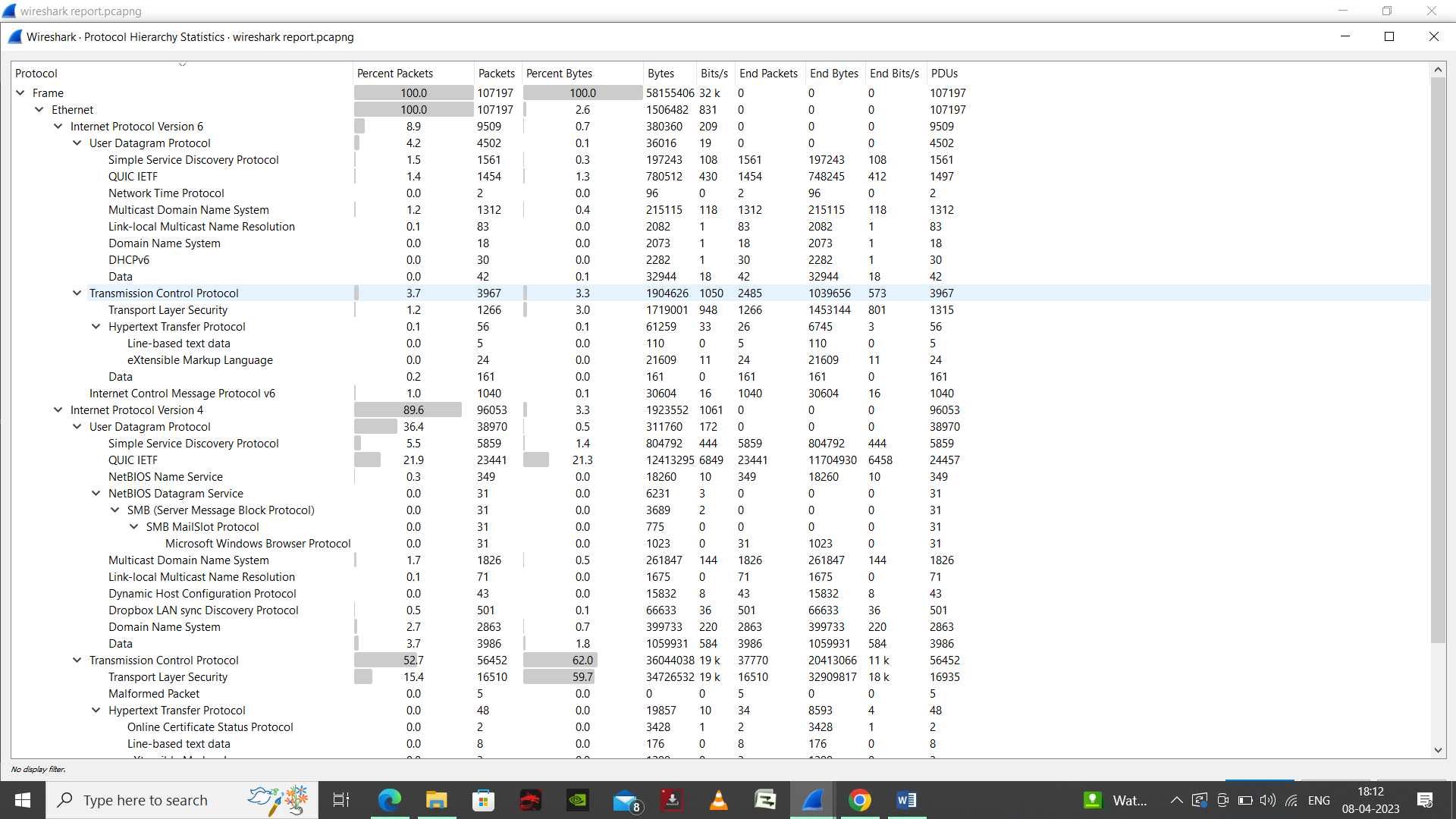
****

Figure.6 Protocol Hierarchy

Protocol Hierarchy in Wireshark provides a summary of the protocols used in a network traffic capture, including the number of packets and bytes used by each protocol. It allows you to quickly analyze the types of traffic on the network and identify any protocol-related issues.

By analyzing the Protocol Hierarchy in Wireshark, you can quickly identify the protocols used in the network traffic capture and their respective usage. This can help you troubleshoot issues related to specific protocols, such as performance problems or compatibility issue

#### This is the final result of the Conversation:

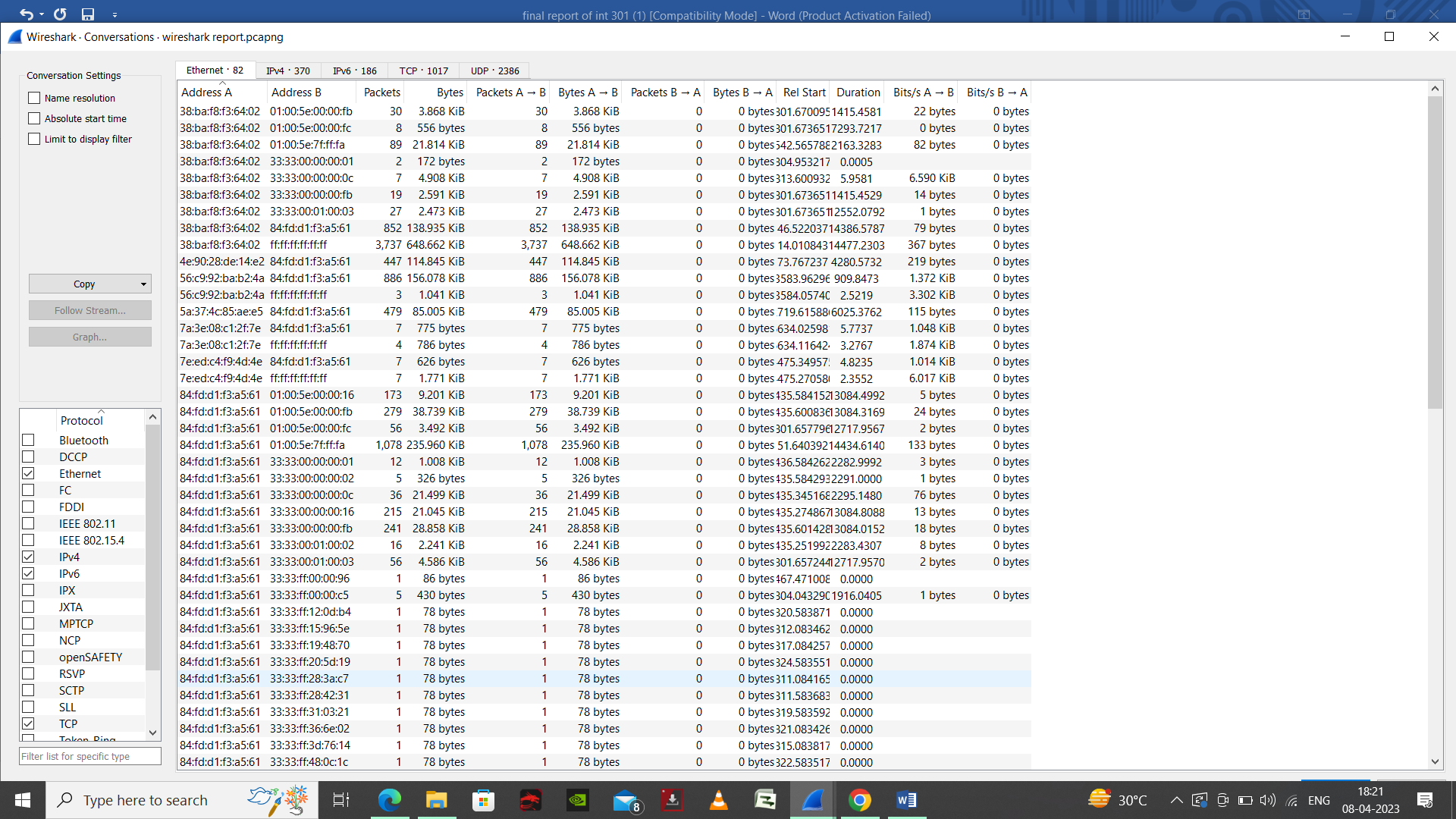
****

Figure.7 Conversations

Conversations feature provides a summary of the communication between pairs of IP addresses in a network traffic capture. It allows you to quickly analyze the traffic patterns and identify any issues related to specific IP addresses or pairs of IP addresses.

By analyzing the conversations in Wireshark, you can quickly identify the IP addresses involved in the network traffic and their respective communication patterns. This can help you troubleshoot issues related to specific IP addresses or pairs of IP addresses, such as performance problems or compatibility issues.

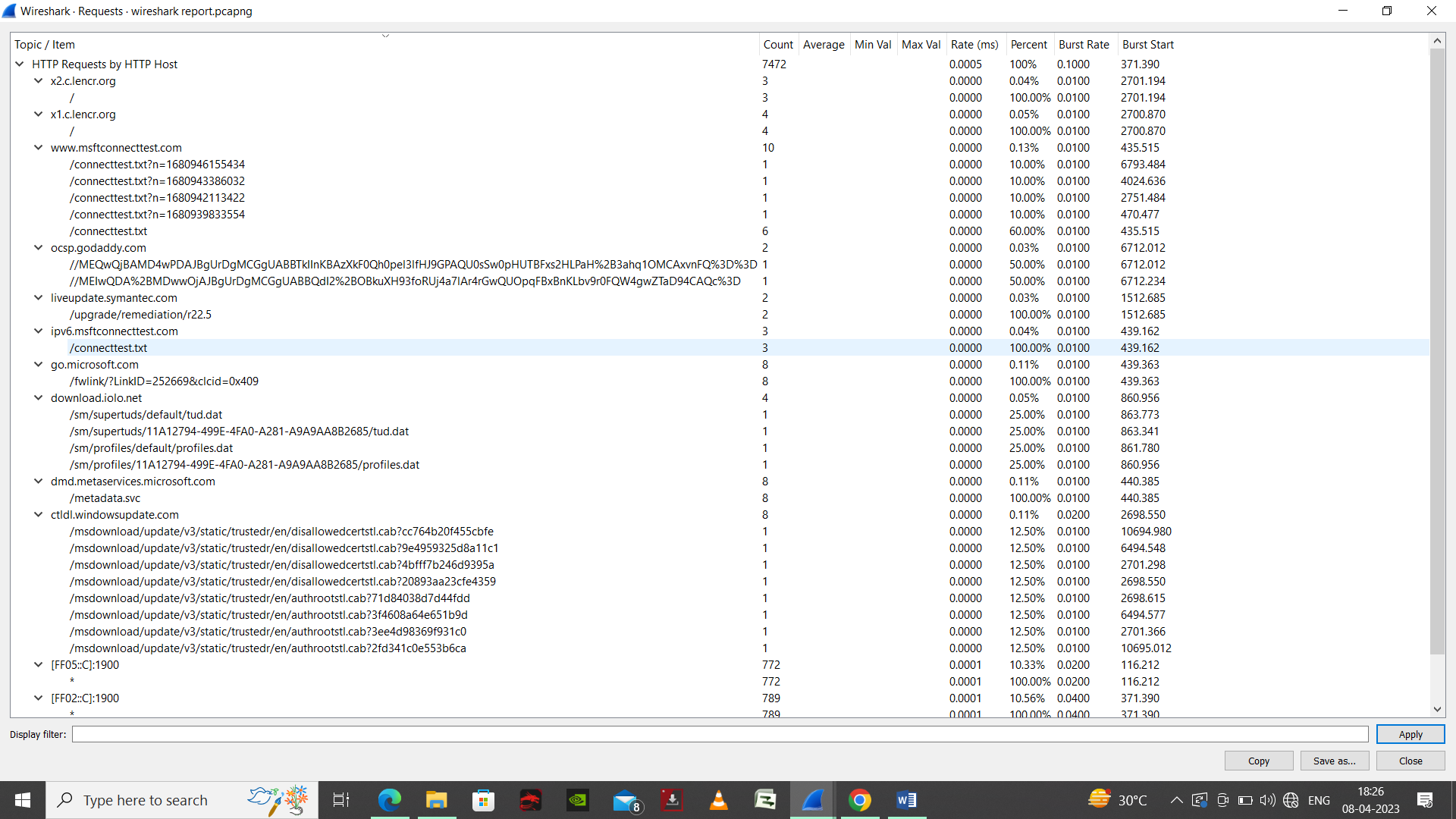


Figure.8 HTTP Request

The HTTP request feature shows the details of each HTTP request made in a network traffic capture. It provides information about the source and destination addresses, the HTTP method used, the requested URL, and other important information related to the request.

By analyzing the HTTP requests in Wireshark, you can gain insights into the types of requests being made, the URLs being accessed, and the performance of the website or application being accessed. This can help you troubleshoot issues related to specific HTTP requests, such as slow performance or errors related to specific URL.

**Reference/ Bibliography**

1. <https://chat.openai.com/chat/01c54247-4aa9-4c08-8c8e-62d5e849776a>
2. <https://www.geeksforgeeks.org/what-is-network-forensics/>
3. <https://www.geeksforgeeks.org/introduction-of-computer-forensics/>
4. <https://www.wireshark.org/download.html>
5. <https://www.geeksforgeeks.org/i-o-graphs-window-in-wireshark/>

**Github-link**