AIM: ANALYZE THE NETWORK TRAFFIC AND PERFORMANCE PARAMETERS OF NETWORK USING WIRESHARK.

THEORY:

Wireshark:

Wireshark is a network or protocol analyser (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyser operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing. Wireshark and other terminal-based free software versions like Tshark are released under the GNU General Public License.

What Does Wireshark Mean?

- ➢ Wireshark is a free and open-source network protocol analyser that enables users to interactively browse the data traffic on a computer network. The development project was started under the name Ethereal, but was renamed Wireshark in 2006.
- ➢ Many networking developers from all around the world have contributed to this project with network analysis, troubleshooting, software development and communication protocols. Wireshark is used in many educational institutions and other industrial sectors.
- ➢ Wireshark shares many characteristics with tcpdump. The difference is that it supports a graphical user interface (GUI) and has information filtering features. In addition, Wireshark permits the user to see all the traffic being passed over the network.
- ➢ Features of Wireshark include:
  - Data is analyzed either from the wire over the network connection or from data files that have already captured data packets.
  - Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
  - With the help of GUI or other versions, users can browse captured data networks.
  - For programmatically editing and converting the captured files to the editcap application, users can use command line switches.
  - Display filters are used to filter and organize the data display.
  - New protocols can be scrutinized by creating plug-ins.

- Captured traffic can also trace Voice over Internet (VoIP) calls over the network.
- When using Linux, it is also possible to capture raw USB traffic.

What Does Network Traffic Mean?

Network traffic refers to the amount of data moving across a network at a given point of time. Network data is mostly encapsulated in network packets, which provide the load in the network. Network traffic is the main component for network traffic measurement, network traffic control and simulation. The proper organization of network traffic helps in ensuring the quality of service in a given network.

Network traffic is also known as data traffic.

Network Traffic:

➢ Network traffic is the main component for bandwidth measurement and management. Moreover, various topologies of the network can only be implemented based on the amount of network traffic in the system.

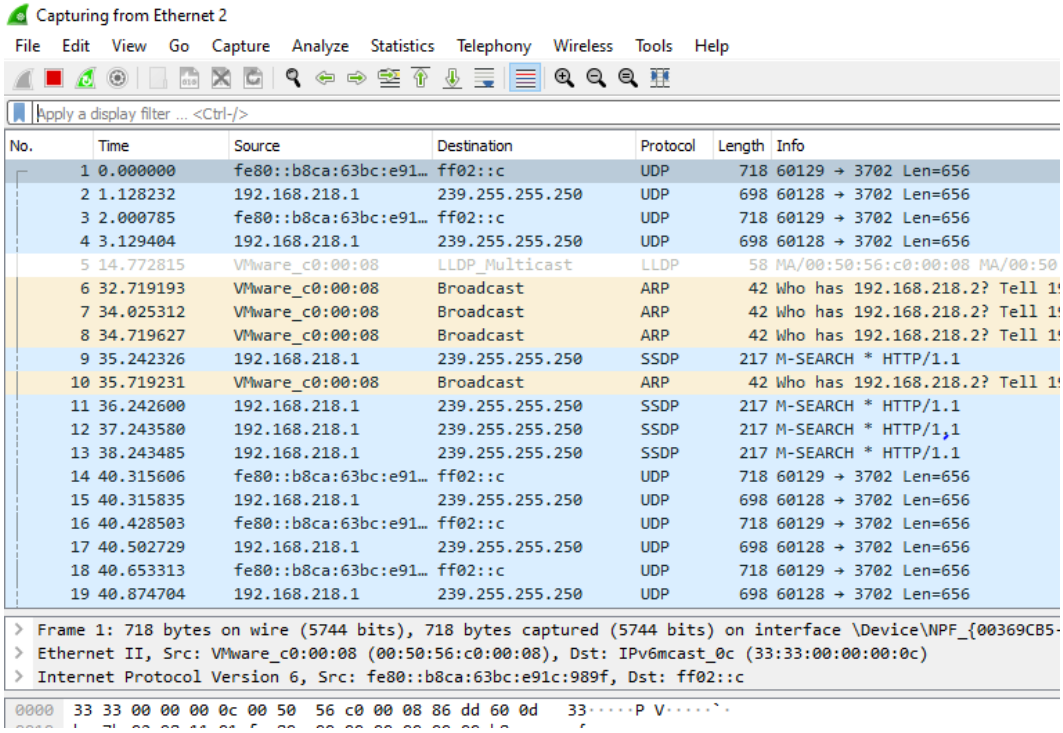
➢ Network traffic can be broadly classified into the following categories:

- Busy/heavy traffic - High bandwidth is consumed in this traffic
- Non-real-time traffic - Consumption of bandwidth during working hours
- Interactive traffic - Is subject to competition for bandwidth and could result in poor response times if prioritization of applications and traffic is not set
- Latency-sensitive traffic - Is subject to competition for bandwidth and could result in poor response times

➢ Proper analysis of network traffic provides the organization with the following benefits:

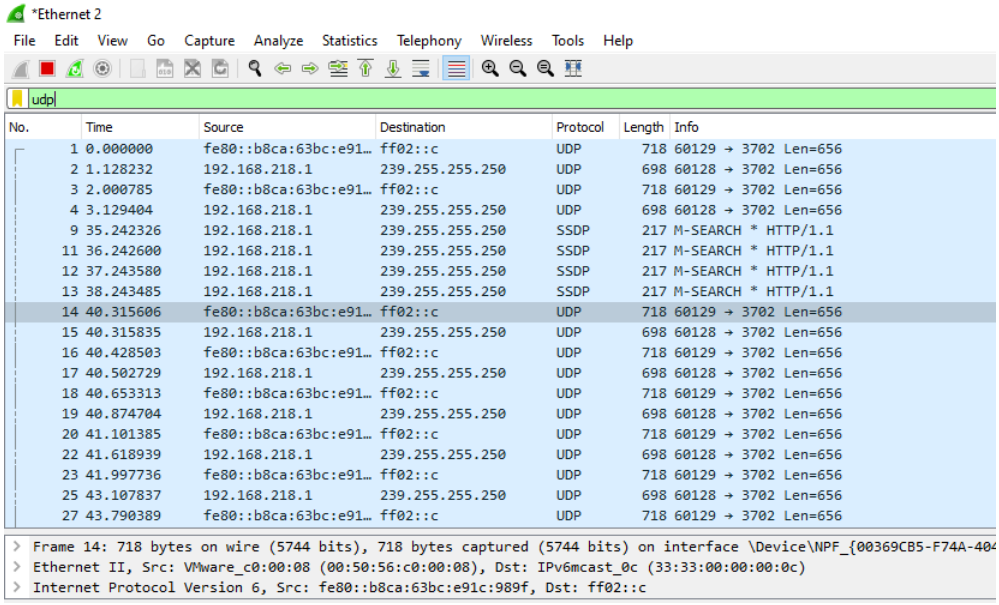
- Identifying network bottlenecks - There could be users or applications that consume high amounts of bandwidth, thus constituting a major part of the network traffic. Different solutions can be implemented to tackle these.
- Network security - unusual amount of traffic in a network is a possible sign of an attack. Network traffic reports provide valuable insights into preventing such attacks.
- Network engineering - Knowing the usage levels of the network allows future requirements to be analyzed.

START CAPTURING:

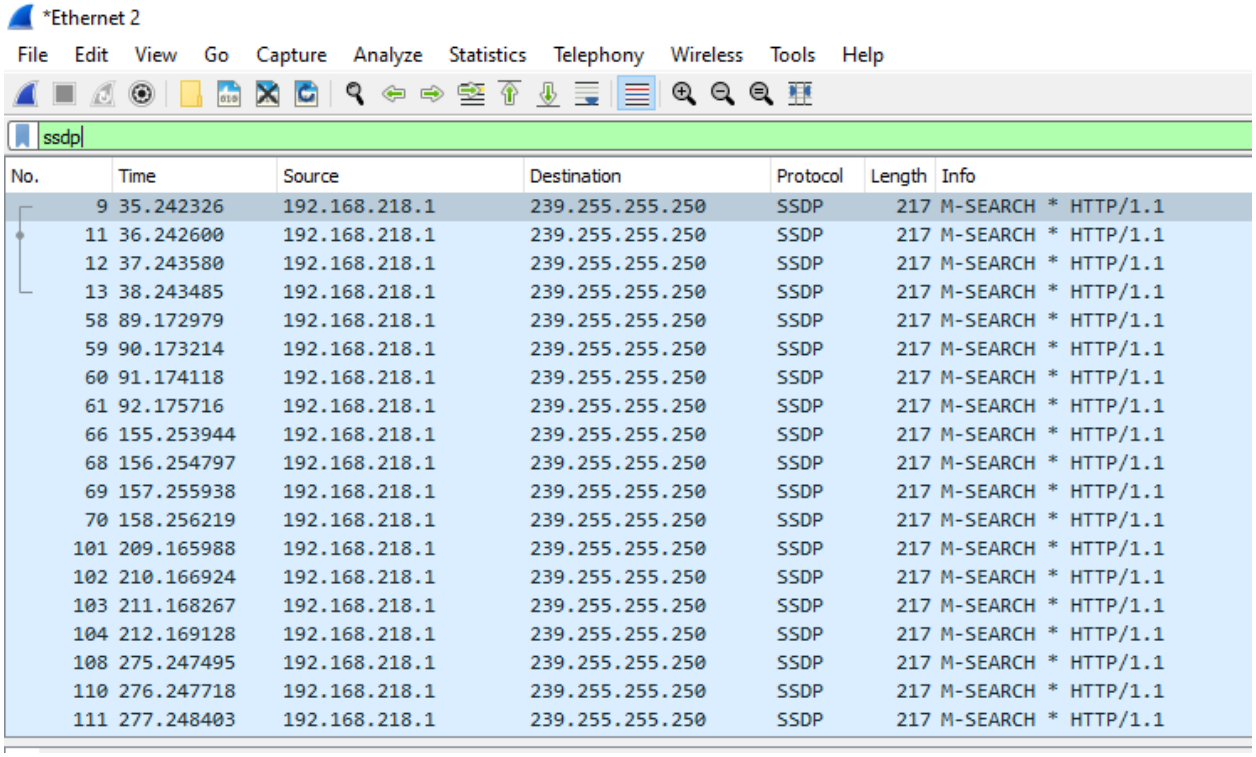


FILTER:

UDP filter:

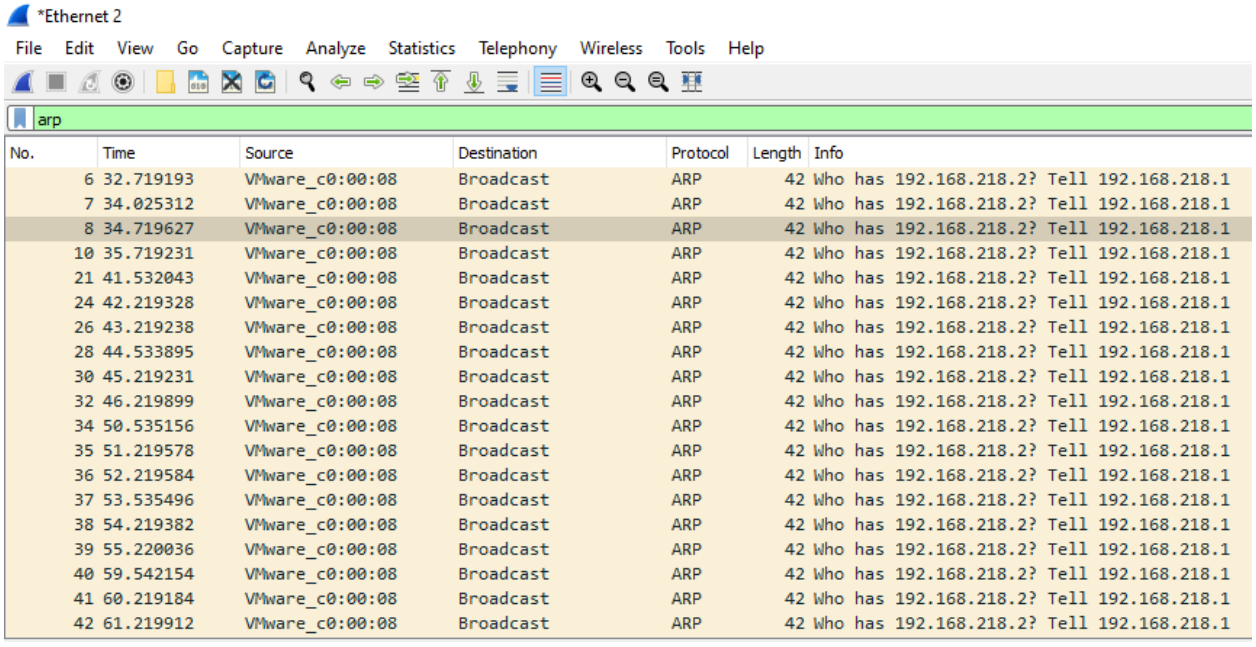


SSDP FILTER:



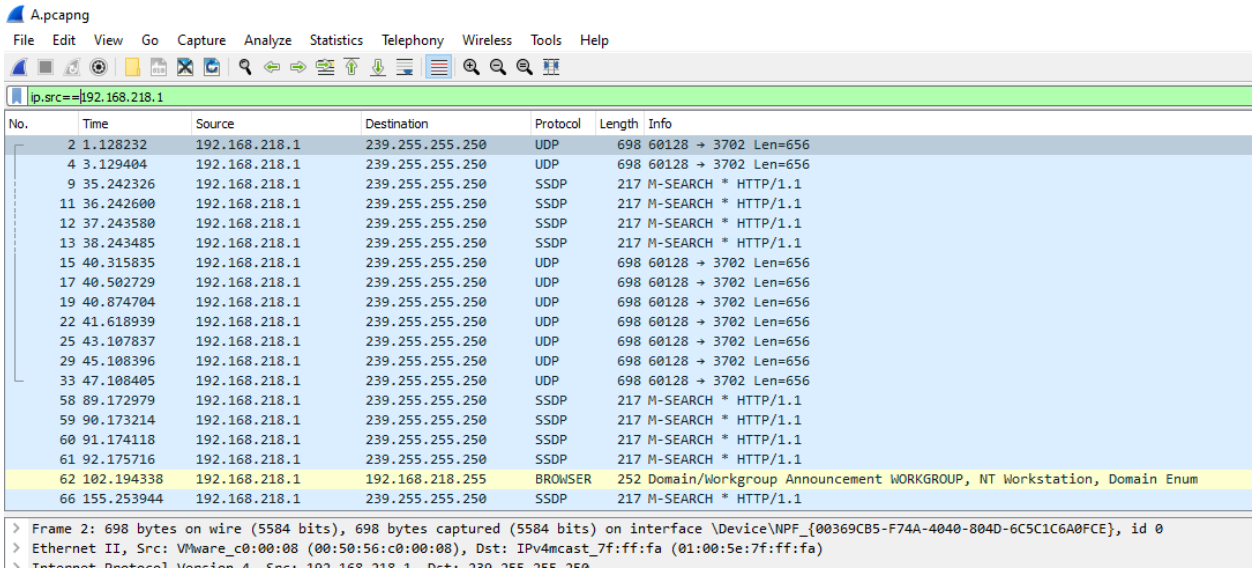
No.	Time	Source	Destination	Protocol	Length	Info
9	35.242326	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
11	36.242600	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	37.243580	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
13	38.243485	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
58	89.172979	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
59	90.173214	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
60	91.174118	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
61	92.175716	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
66	155.253944	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
68	156.254797	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
69	157.255938	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
70	158.256219	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
101	209.165988	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
102	210.166924	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
103	211.168267	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
104	212.169128	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
108	275.247495	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
110	276.247718	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
111	277.248403	192.168.218.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

ARP FILTER:



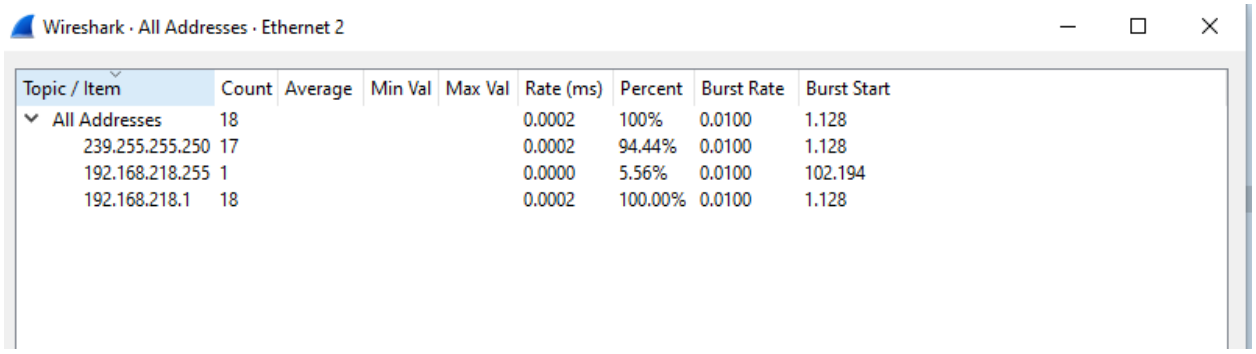
No.	Time	Source	Destination	Protocol	Length	Info
6	32.719193	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
7	34.025312	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
8	34.719627	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
10	35.719231	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
21	41.532043	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
24	42.219328	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
26	43.219238	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
28	44.533895	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
30	45.219231	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
32	46.219899	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
34	50.535156	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
35	51.219578	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
36	52.219584	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
37	53.535496	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
38	54.219382	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
39	55.220036	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
40	59.542154	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
41	60.219184	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1
42	61.219912	VMware_c0:00:08	Broadcast	ARP	42	Who has 192.168.218.2? Tell 192.168.218.1

IP FILTER:

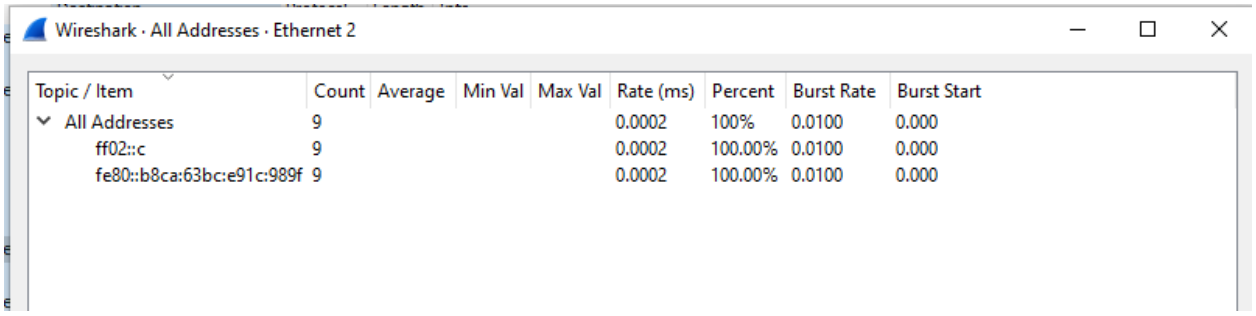


STATS:

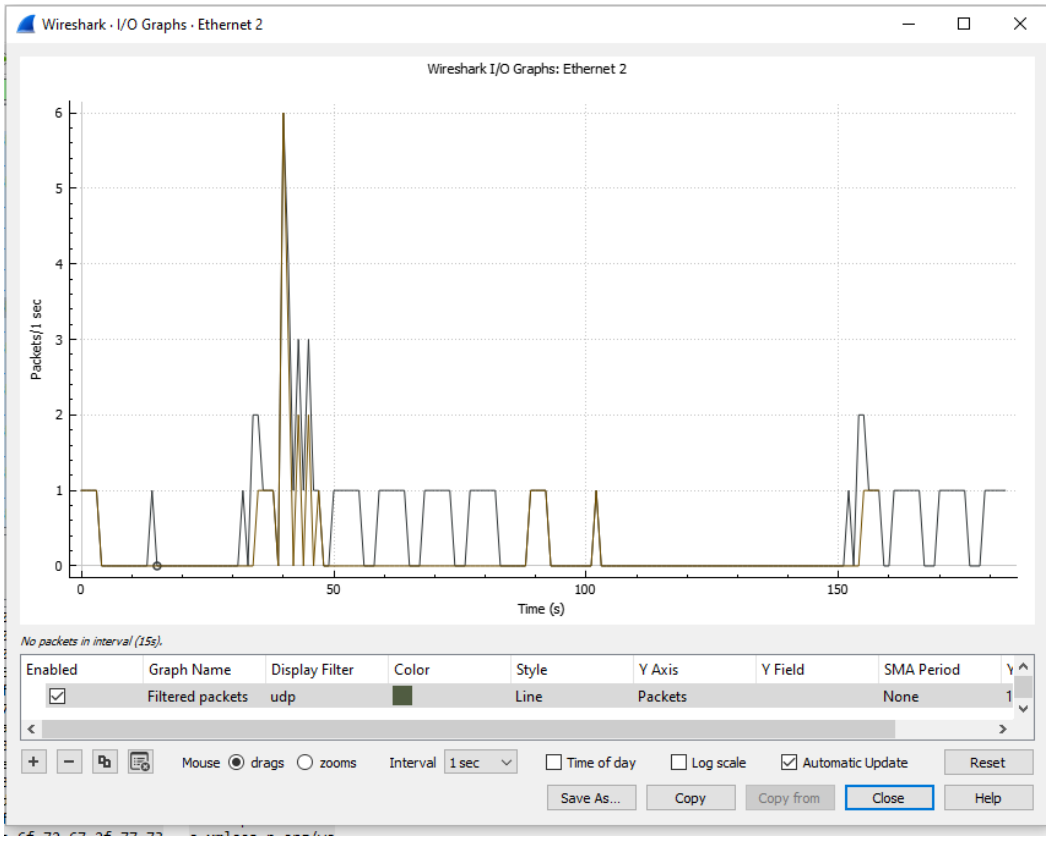
IPV4:



IPV6:



I/O GRAPH:



CONCLUSION:

Analyze the network traffic and performance parameters of the network using Wireshark executed successfully.