INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Network monitoring with open source packet sniffer

Rakhi Shrawat
rakhi.shrawat786@gmail.com
Hindu College of Engineering, Sonepat, Haryana

ABSTRACT

Computer Network is a growing field every day. Networking has made life easy. Computer networks always have a big risk of security problems. However, to better understand real problems in a network and to solve them, it's important to go to the packet level. It is believed that all network problems arise from the packet level. This is where packet analysis plays a big role in computer networks. Network analysis, protocol analysis or simply sniffing are the other names of packet analysis. The purpose of this research paper is to monitor and analyze the network traffic packets of various protocols like TCP/IP, HTTP, ARP, ICMP etc. using a tool called Wireshark. Wireshark is a free and open - source packet analyzer. To analyze the packets of different protocols we are using different parameters are frame no. frame length, IP source, IP destination, header length of the packets and also window size value etc.

Keywords: *Protocols, Wireshark, Packet Flow, Packet Capture, Network Monitoring, Network Analysis, Packet Sniffing.*

1. INTRODUCTION

All network problems start at the core within packets. This is why packet analysis, also referred to as packet sniffing or protocol analysis is used to understand the basics of information traveling across a network. Packet sniffing is used to help maintain a network, comprehend network characteristics, discover who is using a specific network and their peak usage times, and most importantly pinpoint potential malicious attacks and activity. Whenever you connect to the Internet, you are dialing into a network hosted by an Internet Service Provider (ISP) which communicates with other networks. Packet sniffing allows all data within those communications between different ISPs and networks to be viewed, copied, and analyzed. Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues. [1]

2. HISTORY

In the late 1990s, Gerald Combs, a computer science graduate of the University of Missouri–Kansas City, was working for a small Internet service provider.[2] The commercial protocol analysis products at that time were priced around $1500 and did not run on the company's primary platforms (Solaris and Linux), so Combs began writing Ethereal and released the first version around 1998.[3] However, he did not own the Ethereal trademark, so he changed the name to Wireshark.

3. EXPERIMENTAL SETUP

Analysis of the network performance of a given set of websites is done, using Wireshark software as a tool, I have captured packets of websites of the news channel. The set of websites include a website of a news channel and a website for live streaming. I have captured packets of images and audio from the news channel website and I've also captured packets from the live stream website while streaming for 10 minutes on my home network.

4.VARIOUS PROTOCOLS DETECTED IN WIRESHARK FROM A LIVE NETWORK AND WORKING OF THESE PROTOCOLS

While capturing packets from a network interface, Wireshark captures all of the packets coming and going over the network. Wireshark provides capture and display. Filters allow you to specify exactly which packets you have available for analysis. Simply stated, a filter is an expression that defines criteria for the inclusion or exclusion of packets. If there are packets you don't want to see, you can write a filter that gets rid of them. If there are packets you want to see exclusively, you can write a filter that shows only those packets.

Protocols during capturing of the live network:

- TCP/IP,
- HTTP,
- ARP,
- ICMP Protocol.

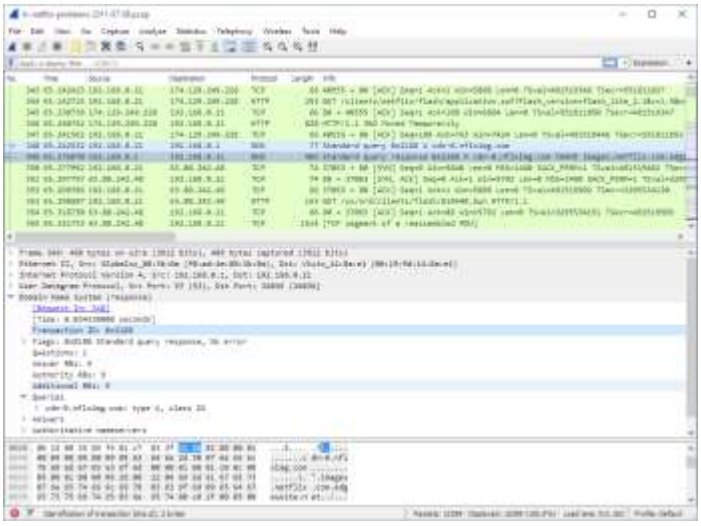

Fig. 1: Wireshark main window showing captured packets

i. TCP/IP

TCP/IP is not a single networking protocol – it is a suite of protocols named after the two most important protocols or layers within it – TCP and IP.TCP/IP is responsible for complete data connectivity and transmitting the data from end to end by providing other functions such as addressing, mapping and acknowledgment. The TCP layer handles the message part. The message is broken down into smaller units, called packets, which are then transmitted over the network. The packets are received by the corresponding TCP layer in the receiver and reassembled into the original message.

The IP layer is primarily concerned with the transmission portion. This is done by means of a unique IP address assigned to each and every active recipient on the network.

To establish a connection, TCP uses a three-way handshake. In the TCP connection establishment sequence, the opening TCP session sends a TCP datagram with the SYN bit set and the receiver sends a related TCP datagram with the SYN ACK bits set. A final ACK bit is sent from a sender to finish the TCP handshake.[4] It is shown in Figure 2. Frame 107 is the start of the three-way handshake whose sequence no. is 0 and after that in packet 111 when it gets acknowledgment from destination its sequence no. gets changed from 0 to 1.

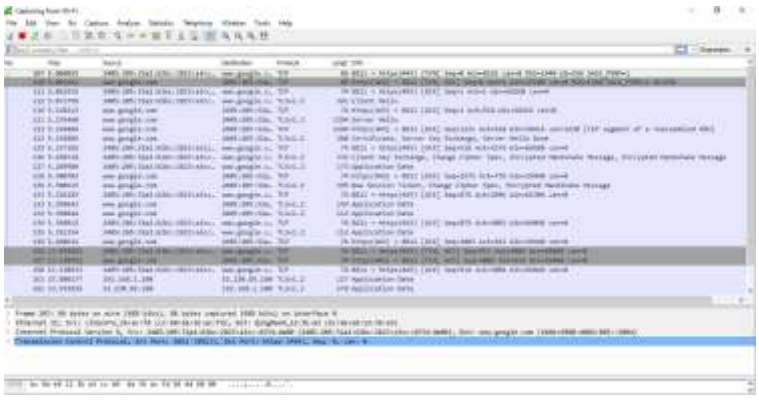

Fig. 2: TCP/IP Protocol connection establishment

Fig. 3: Details of frame 107

Fig. 4: Details of frame 111

ii. HTTP

HTTP functions as a request-response protocol in the client-server computing model. The client submits an HTTP request message to the server. The server, which provides resources such as HTML files and other content, or performs other functions on behalf of the client, returns a response message to the client. The response contains completion status information about the request and may also contain requested content in its message body. [5]

As shown in Figure 4, packet 205 source sends a request to destination for HTTP and in response, it receives GET message in packet 214 after receiving acknowledgment. And at packet 215, the conversation is completed by the HTTP/1.1 message. The Web server responds in HTTP/1.1 with status code ―302 found, which indicates to the browser that the target resource resides temporarily under a different URI.

Fig. 5: HTTP Protocol

As shown in Figure 6, at packet 10551client receives a response in getting the message. At packet 10562 the Web server responds in HTTP/1.1 with status code ―200 OK, which indicates to the browser that the object was successfully fetched

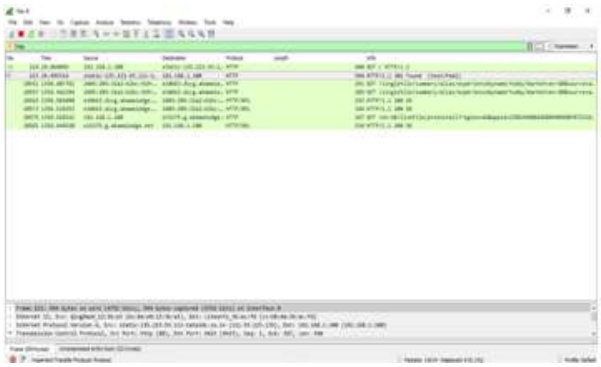

Fig. 6: HTTP Protocol

iii. ARP

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given network layer address, typically an IPv4 address.[6] This mapping is a critical function in the suite. On seeing the capture file seen below in Figure 7, packets collected by it shows in packet no. 518 source computer is sending a packet to IP address 192.168.1.100 asking who has 192.168.1.1 address?

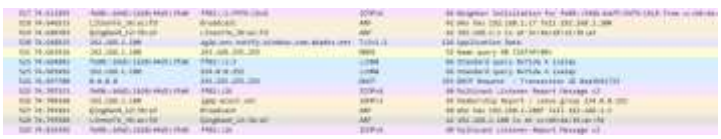

Fig. 7: ARP Protocol asking who has 192.168.1.1 address

In figure 7, ARP Protocol asking who has 192.168.1.1 address it also provides functionality to find client's layer 3 address by allowing transmitting computer to send ARP broadcast. A computer that has IP address will identify itself by sending a response containing its layer 2 address back to transmitting computer. The second packet in Figure 7, Packet 519 shows destination computer's ARP response to the first packet. In response packet no. 519 shows that the above address 192.168.1.1 is at bc:8a:e8:12:3b:a3 machine(MAC address)..If there is no response from the host, it may not be present on the network.

iv. ICMP

The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating [7], as shown in Figure 8, a requested service is not available or that a host or router could not be reached. Computer send echo request, it should receive echo reply in response but in some cases, TTL time exceeded ICMP message is sent when the TTL value of an IP packet reaches zero. In normal operation, a network should not have a diameter so great that the TTL gets reduced to zero. The most common occurrence of this is when there is a routing loop. In this case, as the packet is sent back and forth between the looping points, the TTL keeps getting decremented until it reaches zero. That's when this message is sent.

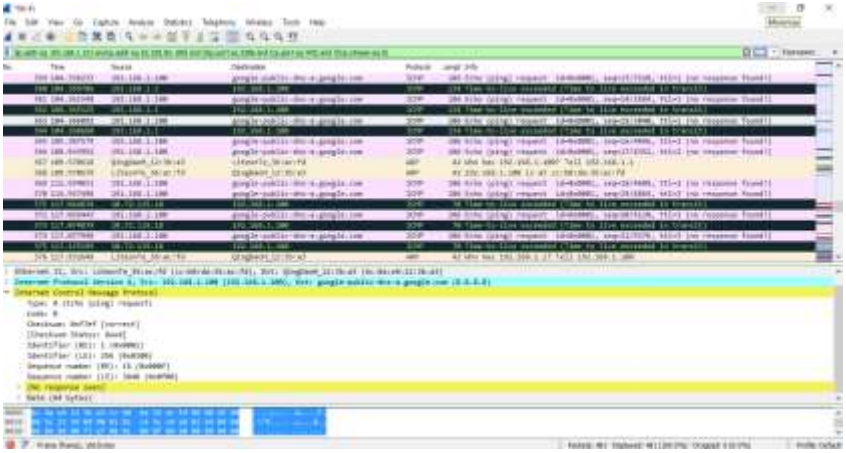

Fig. 8: ICMP Protocol

5. GRAPHS AND OTHER PROPERTIES RELATED TO THE CAPTURED PACKETS

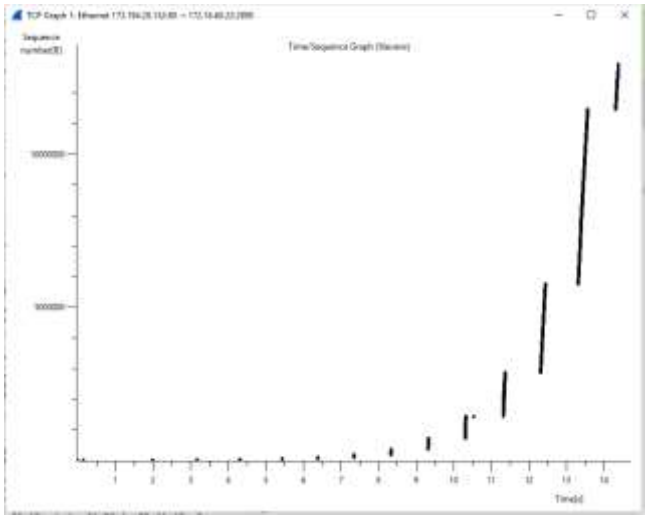

Fig. 9: Time Sequence Graph of the captured packets

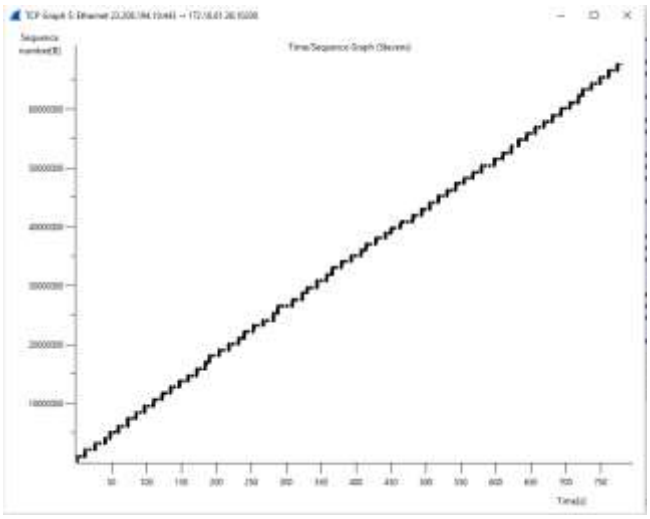

Fig. 10: Time Sequence Graph of the captured packets

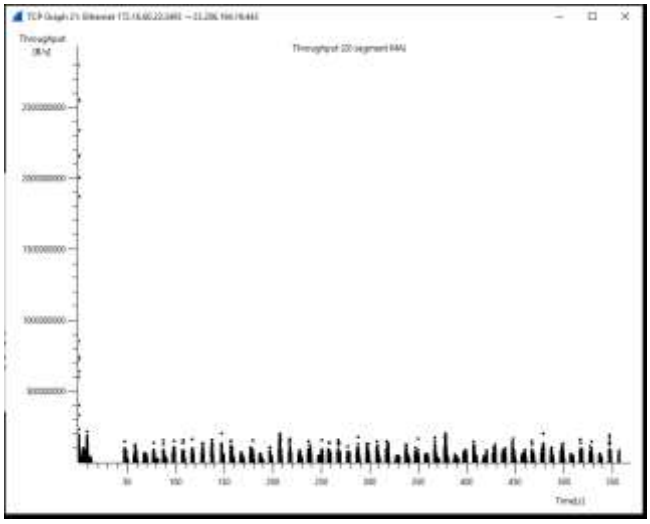

Fig. 11: Throughput Graph of the captured packets

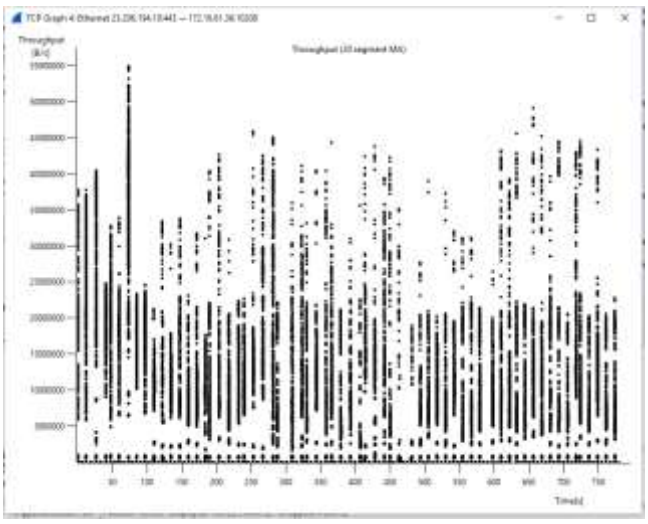

Fig. 12: Throughput Graph of the captured packets

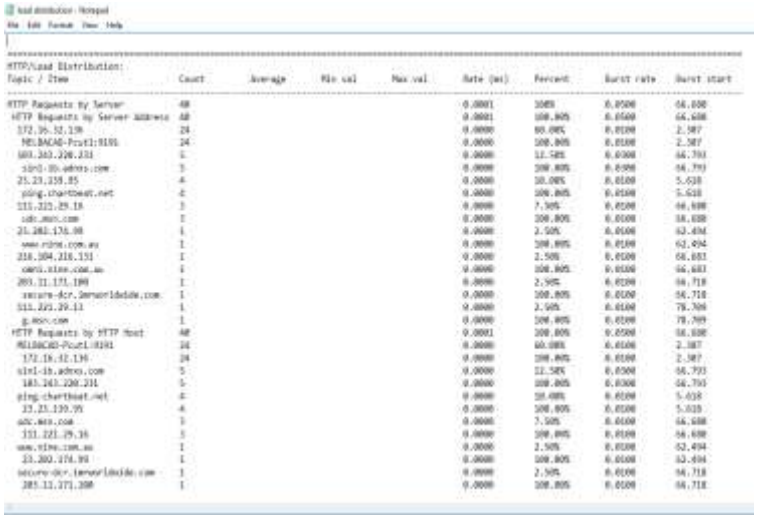

Fig. 13: Load Distribution of the captured packets

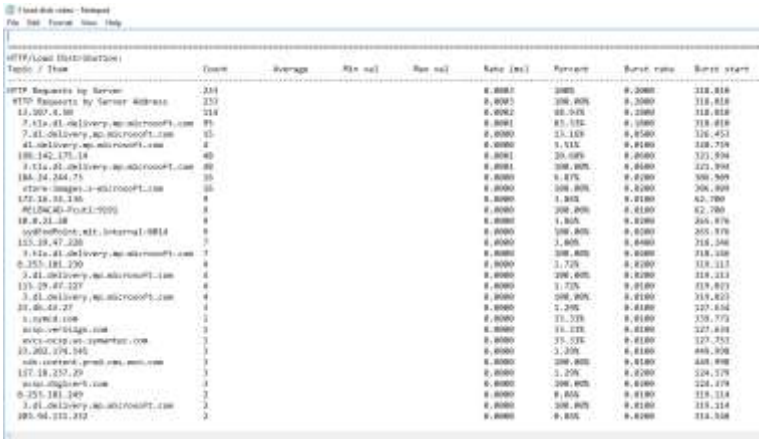

Fig. 14: Load Distribution of the captured packets

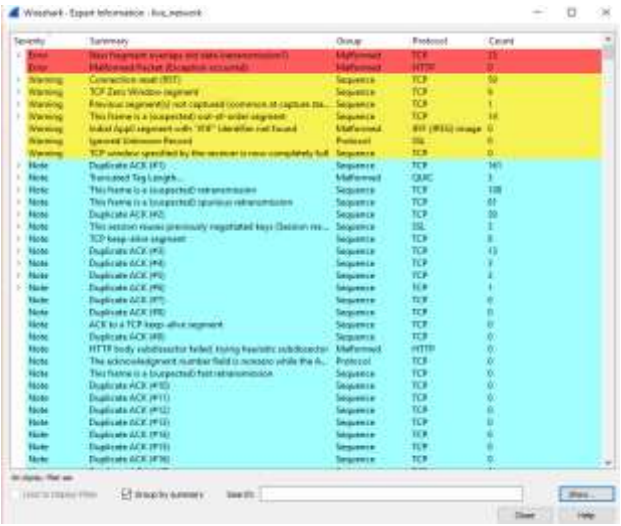

Fig. 15: Expert Information showing duplicate packets

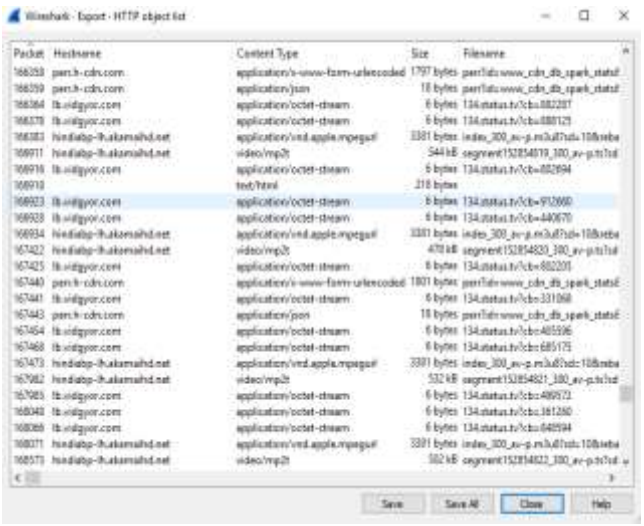

Fig. 16: HTTP Object List

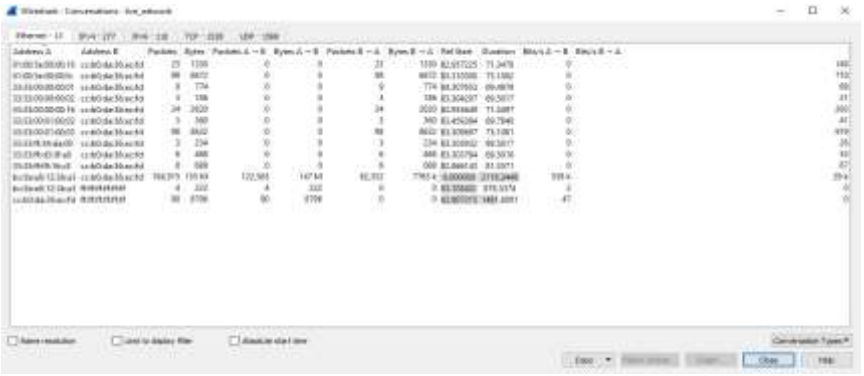

Fig. 17: Conversation Window

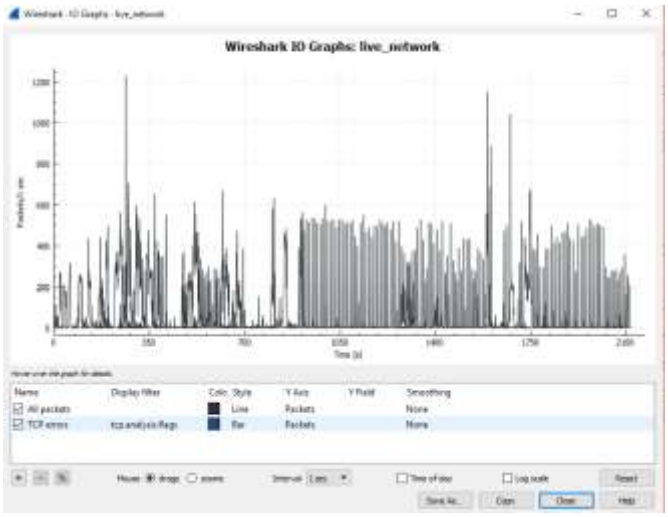

Fig. 18: I/O Graph of captured packets

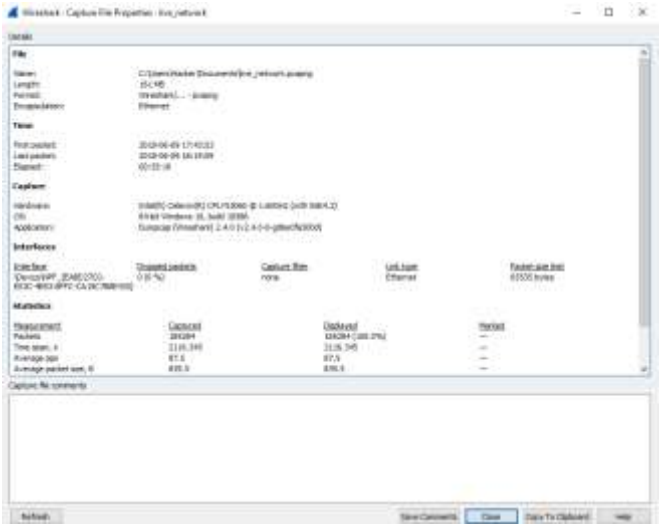

Fig. 19: Capture File Properties Window

6. CONCLUSION

In this paper network traffic from a live network is shown by monitoring and analysis on that captured files and then statistics is built. Using Wireshark software was easy and convenient as it gave me a real understanding of network performance. Wireshark gives an option in which we get the object list of the packets we captured or say a user who is on the network using whatever sites they visit. Various graphs related to captured files are shown and other attractive features are shown which make Wireshark a great tool for network analysis. Among all the properties listed above, the most interesting one was Load Distribution. The output graphs generated through captured packets provides details of network performance. This paper helps in the practical understanding of network performance and applications.

7. REFERENCES

[1] En.wikipedia.org. (2018). Wireshark. [online] Available at: https://en.wikipedia.org/wiki/Wireshark [Accessed 5 Apr. 2018].
[2] Wireshark.org. (2018). 1.4. A brief history of Wireshark. [online] Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html [Accessed 15 Apr. 2018].
[3] Wireshark.org. (2018). 1.4. A brief history of Wireshark. [online] Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html [Accessed 15 Apr. 2018].
[4] Tcpipguide.com. (2018). The TCP/IP Guide - TCP Connection Establishment Process: The "Three-Way Handshake". [online] Available at: http://www.tcpipguide.com/free/t_TCPConnectionEstablishmentProcessTheThreeWayHandsh-3.htm [Accessed 19 May. 2018].
[5] En.wikipedia.org. (2018). Hypertext Transfer Protocol. [online] Available at: https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol [Accessed 21 May. 2018].
[6] En.wikipedia.org. (2018). Address Resolution Protocol. [online] Available at: https://en.wikipedia.org/wiki/Address_Resolution_Protocol [Accessed 21 May. 2018].
[7] En.wikipedia.org. (2018). Internet Control Message Protocol. [online] Available at: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol [Accessed 22 May. 2018].

