Name:	Prerna Sunil Jadhav
Sap Id:	60004220127
Class:	S. Y. B.Tech (Computer Engineering)
Course:	Computer Networks (DJ12CEL405)
Date of Performance:	
Date of Submission:	
Experiment No.:	09
Aim:	Packet Capturing In Wireshark

AIM: TO IMPLEMENT AND SIMULATE PACKET CAPTURING IN WIRESHARK.

THEORY:

- ✓ A packet is a unit of data which is transmitted over a network between the origin and the destination.
- ✓ Network packets are small, i.e., maximum 1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets. The data packets in the Wireshark can be viewed online and can be analyzed offline.
- ✓ Packet capturing and analyzing are essential tasks in computer networking, especially in troubleshooting network problems and securing the network from malicious attacks. Here are some notes on packet capturing and analyzing in computer networking:
    - Packet capturing: Packet capturing is the process of intercepting and collecting network traffic data packets for analysis. Packet capturing tools are used to capture packets passing through a specific network interface. Some popular packet capturing tools include Wireshark, tcpdump, and Microsoft Network Monitor.
    - Packet analysis: Packet analysis involves examining the captured packets to understand the network traffic patterns, identify issues, and pinpoint the source of problems. Packet analysis tools are used to analyze the captured packets to gain insight into the network traffic, identify performance issues, and detect potential security threats. Some popular packet analysis tools include Wireshark, Microsoft Message Analyzer, and Network Miner.
    - Protocols: Network traffic consists of packets of data that are exchanged between different devices using different protocols. Popular protocols include TCP, UDP, HTTP, DNS, SMTP, FTP, and ICMP. Understanding the protocols used in network traffic is essential to perform effective packet analysis.
    - Filters: Packet filtering is the process of selecting and analyzing packets based on specific criteria. Packet filtering tools allow users to filter packets based on protocols, source and destination addresses, port numbers, and other parameters. This helps in isolating specific packets for analysis and improving the efficiency of packet analysis.
    - Security: Packet capturing and analysing can also be used for security purposes, such as detecting and preventing cyber-attacks. Network administrators can use packet

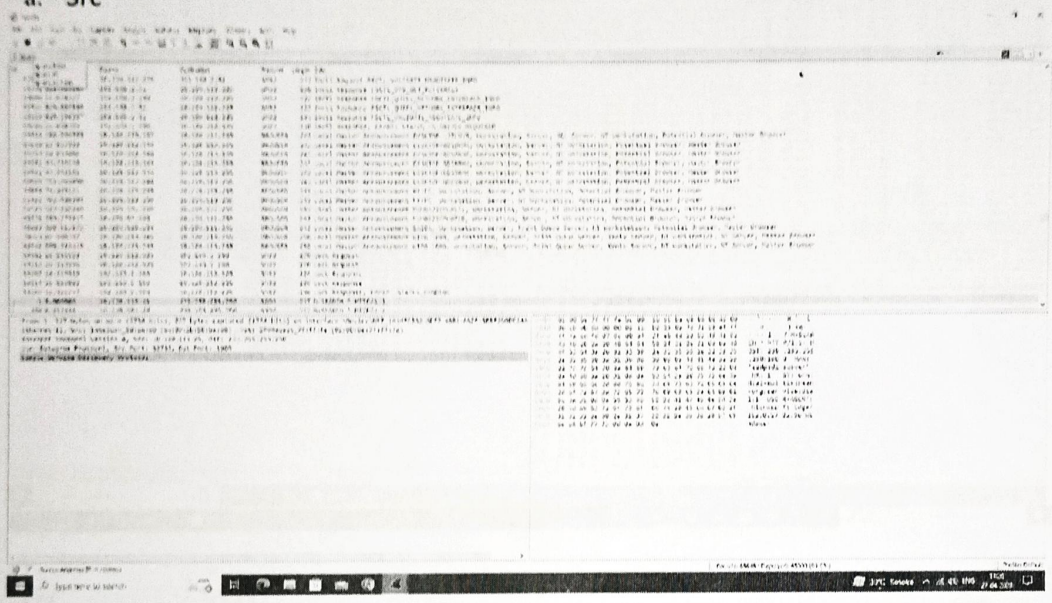
analysis to identify and block malicious traffic, analyse security threats, and detect intrusions.

- ✓ Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.
- ✓ It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.
- ✓ Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.
- ✓ Uses of Wireshark:
  1. It is used by network security engineers to examine security problems.
  2. It allows the users to watch all the traffic being passed over the network.
  3. It is used by network engineers to troubleshoot network issues.
  4. It also helps to troubleshoot latency issues and malicious activities on your network.
  5. It can also analyze dropped packets.
  6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

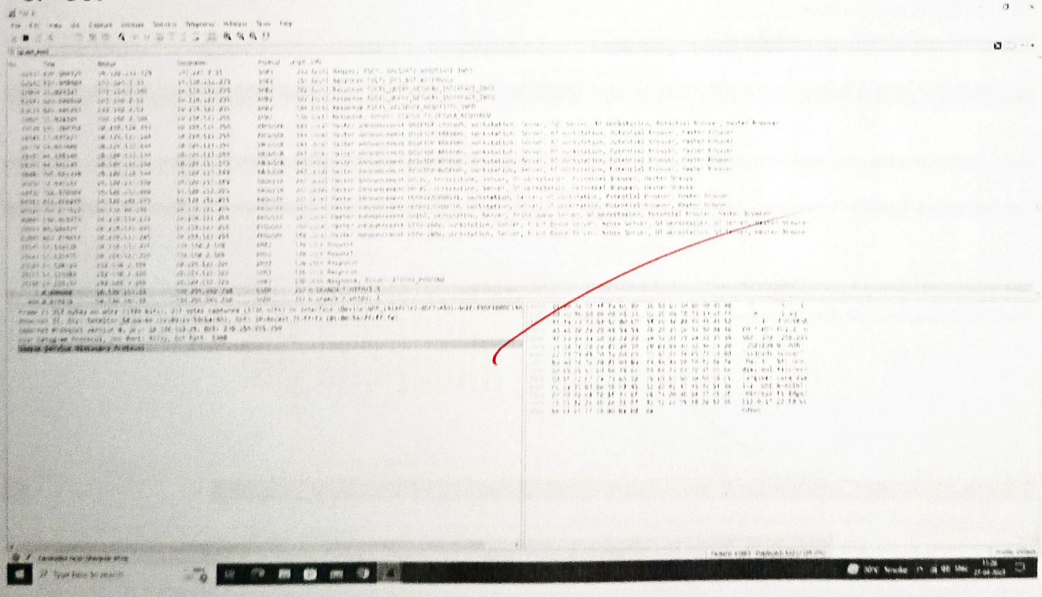
R 415

Filters in Wireshark

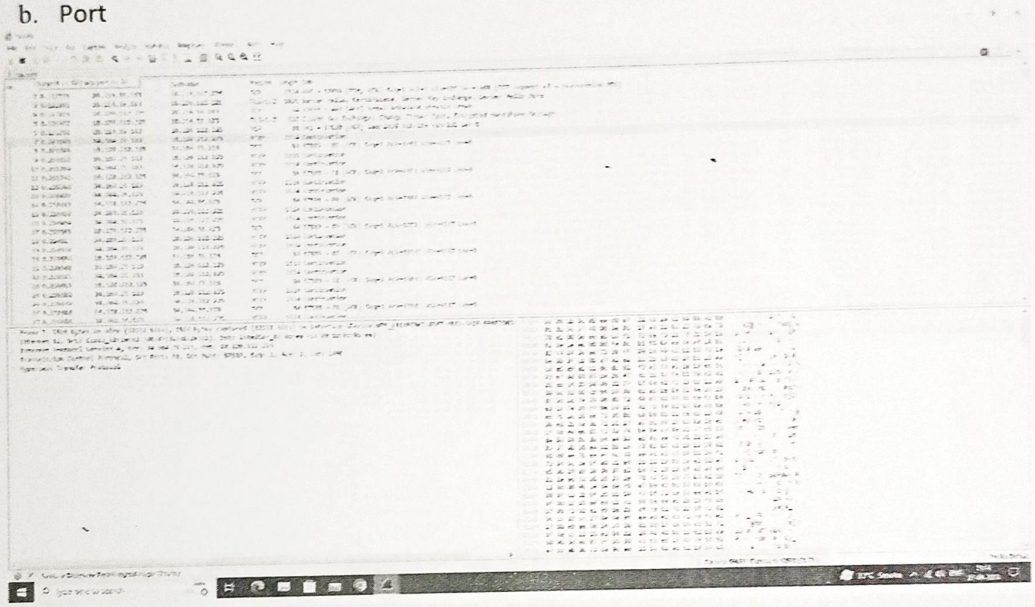
1. Ip:
   a. Src



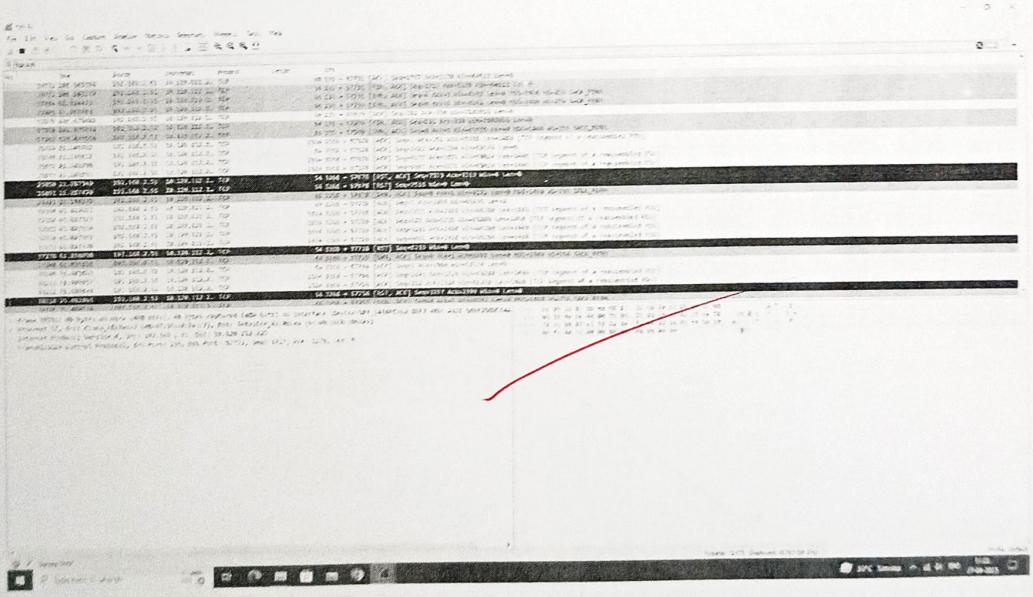
   b. Dst



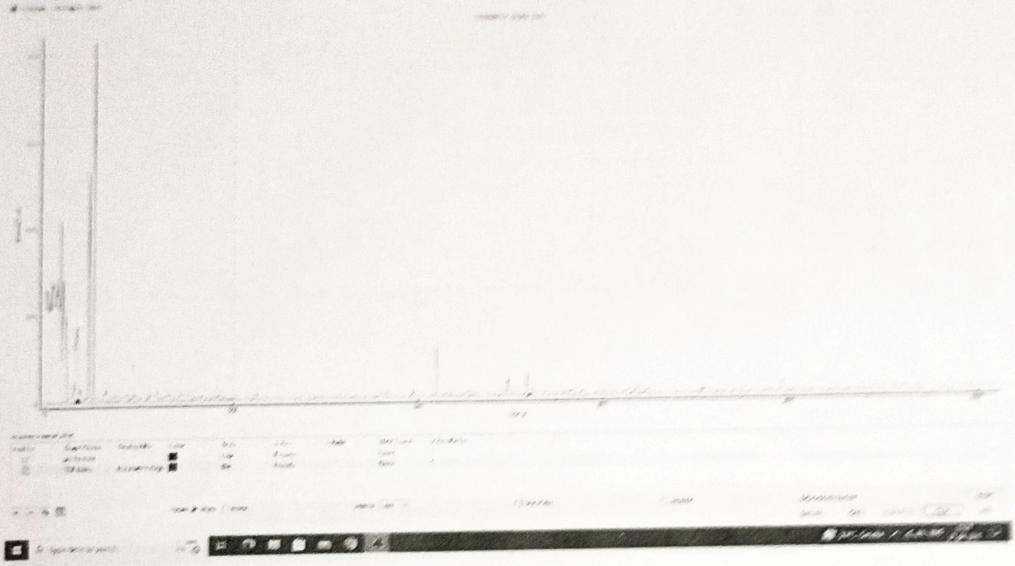
b. Port



c. Ack



6. I/O Graph:



Conclusion: Thus, we have simulated Packet Capturing in Wireshark.

9415