



Academic Year: 2022-2023

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



Academic Year: 2022-2023

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.

R415



Academic Year: 2022-2023

Filters in Wireshark

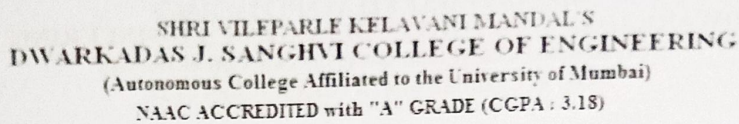
1. Ip:

a. Src

Wireshark packet capture showing IP source filters. The packet list shows various IP addresses. The packet details pane shows the selected packet's structure. The packet bytes pane shows the raw data. The filter bar at the top shows the active filter: ip.src == 192.168.1.100. The packet list is filtered to show only packets from 192.168.1.100.

b. Dst

Wireshark packet capture showing IP destination filters. The packet list shows various IP addresses. The packet details pane shows the selected packet's structure. The packet bytes pane shows the raw data. The filter bar at the top shows the active filter: ip.dst == 192.168.1.100. The packet list is filtered to show only packets to 192.168.1.100.



b. Port

[illegible]

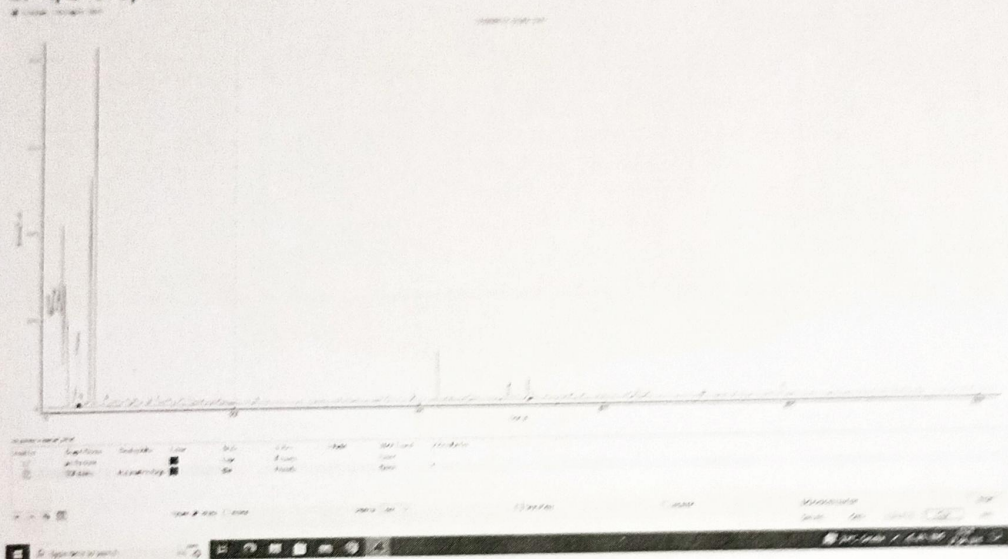
c. Ack

The image is a screenshot of a Windows XP desktop. The primary focus is a Notepad++ window titled "Untitled - Notepad++" which contains a list of IP addresses, likely from a network scan. The text is as follows:

```
192.168.1.1  
192.168.1.2  
192.168.1.3  
192.168.1.4  
192.168.1.5  
192.168.1.6  
192.168.1.7  
192.168.1.8  
192.168.1.9  
192.168.1.10  
192.168.1.11  
192.168.1.12  
192.168.1.13  
192.168.1.14  
192.168.1.15  
192.168.1.16  
192.168.1.17  
192.168.1.18  
192.168.1.19  
192.168.1.20  
192.168.1.21  
192.168.1.22  
192.168.1.23  
192.168.1.24  
192.168.1.25  
192.168.1.26  
192.168.1.27  
192.168.1.28  
192.168.1.29  
192.168.1.30  
192.168.1.31  
192.168.1.32  
192.168.1.33  
192.168.1.34  
192.168.1.35  
192.168.1.36  
192.168.1.37  
192.168.1.38  
192.168.1.39  
192.168.1.40  
192.168.1.41  
192.168.1.42  
192.168.1.43  
192.168.1.44  
192.168.1.45  
192.168.1.46  
192.168.1.47  
192.168.1.48  
192.168.1.49  
192.168.1.50  
192.168.1.51  
192.168.1.52  
192.168.1.53  
192.168.1.54  
192.168.1.55  
192.168.1.56  
192.168.1.57  
192.168.1.58  
192.168.1.59  
192.168.1.60  
192.168.1.61  
192.168.1.62  
192.168.1.63  
192.168.1.64  
192.168.1.65  
192.168.1.66  
192.168.1.67  
192.168.1.68  
192.168.1.69  
192.168.1.70  
192.168.1.71  
192.168.1.72  
192.168.1.73  
192.168.1.74  
192.168.1.75  
192.168.1.76  
192.168.1.77  
192.168.1.78  
192.168.1.79  
192.168.1.80  
192.168.1.81  
192.168.1.82  
192.168.1.83  
192.168.1.84  
192.168.1.85  
192.168.1.86  
192.168.1.87  
192.168.1.88  
192.168.1.89  
192.168.1.90  
192.168.1.91  
192.168.1.92  
192.168.1.93  
192.168.1.94  
192.168.1.95  
192.168.1.96  
192.168.1.97  
192.168.1.98  
192.168.1.99  
192.168.1.100  
192.168.1.101  
192.168.1.102  
192.168.1.103  
192.168.1.104  
192.168.1.105  
192.168.1.106  
192.168.1.107  
192.168.1.108  
192.168.1.109  
192.168.1.110  
192.168.1.111  
192.168.1.112  
192.168.1.113  
192.168.1.114  
192.168.1.115  
192.168.1.116  
192.168.1.117  
192.168.1.118  
192.168.1.119  
192.168.1.120  
192.168.1.121  
192.168.1.122  
192.168.1.123  
192.168.1.124  
192.168.1.125  
192.168.1.126  
192.168.1.127  
192.168.1.128  
192.168.1.129  
192.168.1.130  
192.168.1.131  
192.168.1.132  
192.168.1.133  
192.168.1.134  
192.168.1.135  
192.168.1.136  
192.168.1.137  
192.168.1.138  
192.168.1.139  
192.168.1.140  
192.168.1.141  
192.168.1.142  
192.168.1.143  
192.168.1.144  
192.168.1.145  
192.168.1.146  
192.168.1.147  
192.168.1.148  
192.168.1.149  
192.168.1.150  
192.168.1.151  
192.168.1.152  
192.168.1.153  
192.168.1.154  
192.168.1.155  
192.168.1.156  
192.168.1.157  
192.168.1.158  
192.168.1.159  
192.168.1.160  
192.168.1.161  
192.168.1.162  
192.168.1.163  
192.168.1.164  
192.168.1.165  
192.168.1.166  
192.168.1.167  
192.168.1.168  
192.168.1.169  
192.168.1.170  
192.168.1.171  
192.168.1.172  
192.168.1.173  
192.168.1.174  
192.168.1.175  
192.168.1.176  
192.168.1.177  
192.168.1.178  
192.168.1.179  
192.168.1.180  
192.168.1.181  
192.168.1.182  
192.168.1.183  
192.168.1.184  
192.168.1.185  
192.168.1.186  
192.168.1.187  
192.168.1.188  
192.168.1.189  
192.168.1.190  
192.168.1.191  
192.168.1.192  
192.168.1.193  
192.168.1.194  
192.168.1.195  
192.168.1.196  
192.168.1.197  
192.168.1.198  
192.168.1.199  
192.168.1.200  
192.168.1.201  
192.168.1.202  
192.168.1.203  
192.168.1.204  
192.168.1.205  
192.168.1.206  
192.168.1.207  
192.168.1.208  
192.168.1.209  
192.168.1.210  
192.168.1.211  
192.168.1.212  
192.168.1.213  
192.168.1.214  
192.168.1.215  
192.168.1.216  
192.168.1.217  
192.168.1.218  
192.168.1.219  
192.168.1.220  
192.168.1.221  
192.168.1.222  
192.168.1.223  
192.168.1.224  
192.168.1.225  
192.168.1.226  
192.168.1.227  
192.168.1.228  
192.168.1.229  
192.168.1.230  
192.168.1.231  
192.168.1.232  
192.168.1.233  
192.168.1.234  
192.168.1.235  
192.168.1.236  
192.168.1.237  
192.168.1.238  
192.168.1.239  
192.168.1.240  
192.168.1.241  
192.168.1.242  
192.168.1.243  
192.168.1.244  
192.168.1.245  
192.168.1.246  
192.168.1.247  
192.168.1.248  
192.168.1.249  
192.168.1.250  
192.168.1.251  
192.168.1.252  
192.168.1.253  
192.168.1.254  
192.168.1.255  
192.168.1.256  
192.168.1.257  
192.168.1.258  
192.168.1.259  
192.168.1.260  
192.168.1.261  
192.168.1.262  
192.168.1.263  
192.168.1.264  
192.168.1.265  
192.168.1.266  
192.168.1.267  
192.168.1.268  
192.168.1.269  
192.168.1.270  
192.168.1.271  
192.168.1.272  
192.168.1.273  
1
```




6. I/O Graph:



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

9415