

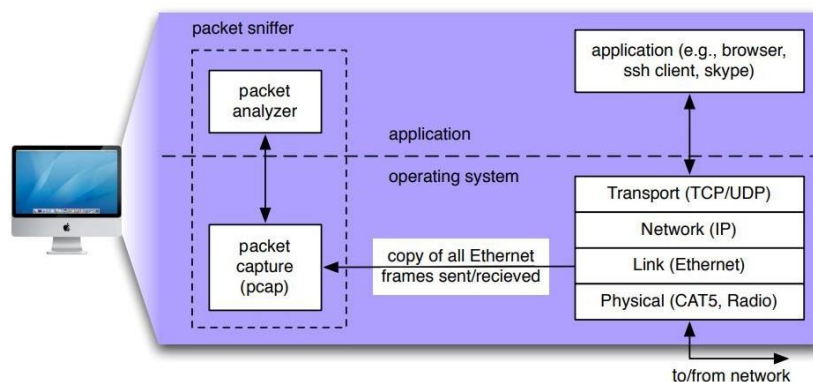


Experiment No: 09

Aim: Simulate Packet Capturing in Wireshark

Theory:

- Packet sniffers are a basic tool for observing the messages on a network. As the name suggests, a packet sniffer captures ("sniffs") messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine.



- The figure above shows the structure of a packet sniffer. At the right are the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle, is an addition to the usual software in your computer and consists of two parts. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer. As you know, messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In the figure, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.
- The existence of the packet capture box in this figure should give you cause to pause and think, particularly down two trains of thought. Firstly, it shows that any packet in a shared medium (Ethernet, Wi-Fi, etc) can be captured and examined without notification of the sender or receiver. You cannot rely on common link-layer protocols to protect your secrets or your privacy online. At a minimum, you should be using encryption protocols (generally buried



Department of Computer Engineering
Class: S.Y. B.Tech. Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

in the application layer, though sometimes found elsewhere) to protect all network traffic you generate or receive. Secondly, you have the ability to act as the "bad guy" and capture the network traffic of other people, examine it and exploit what you find.

- The second component of a packet sniffer is the packet analyzer, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols. For example, suppose we are interested in displaying the various fields in messages exchanged by the HTTP protocol. The packet analyzer understands the format of Ethernet frames, and so can identify the IP datagram within an Ethernet frame. It also understands the IP datagram format, so that it can extract the TCP segment within the IP datagram. Finally, it understands the TCP segment structure, so it can extract the HTTP message contained in the TCP segment. Finally, it understands the HTTP protocol and so, for example, knows that the first bytes of an HTTP message will contain the string "GET," "POST," or "HEAD".
- We will be using the Wireshark packet sniffer, allowing us to display the contents of messages being sent/received from/by protocols at different levels of the protocol stack. (Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer). Wireshark is a free network protocol analyzer that runs on Macintosh, Windows, and Linux/Unix computers. It's an ideal packet analyzer for our labs – it is stable, has a large user base and well-documented support that includes a userguide, man pages, and a detailed FAQ, rich functionality that includes the capability to analyze hundreds of protocols, and a well-designed user interface. It operates in computers using Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LANs, and ATM connections (if the OS on which it's running allows Wireshark to do so).



**SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)



NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

Department of Computer Engineering
Class: S.Y. B.Tech. Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

Working:

Filters in Wireshark

1. Ip:
 - a. Src

The screenshot shows a Wireshark packet capture on the 'Wi-Fi' interface. The packet list on the left shows a series of SYN packets from 192.168.2.51 to 192.168.2.100. The packet details pane shows the 'Ethernet II' and 'Internet Protocol Version 4' sections. The 'Internet Protocol Version 4' section shows the source IP as 192.168.2.51 and the destination IP as 192.168.2.100. The packet bytes pane shows the raw data of the packet.

- b. Dst

The screenshot shows a Wireshark packet capture on the 'Wi-Fi' interface. The packet list on the left shows a series of SYN packets from 192.168.2.51 to 192.168.2.100. The packet details pane shows the 'Ethernet II' and 'Internet Protocol Version 4' sections. The 'Internet Protocol Version 4' section shows the source IP as 192.168.2.51 and the destination IP as 192.168.2.100. The packet bytes pane shows the raw data of the packet.



**SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



Department of Computer Engineering
Class: S.Y. B.Tech.

Course Code: DJ19CEL405

Semester: IV
Course Name: Computer Networks Lab

c. Addr

Wireshark packet capture showing ARP request and response. The packet list shows an ARP request from 10.128.112.225 to 10.128.112.255. The packet details show the Ethernet II, Internet Protocol Version 4, and ARP (Request) fields. The packet bytes show the raw data in hexadecimal and ASCII.

2. Tcp:

a. Tcp

Wireshark packet capture showing TCP connection establishment. The packet list shows a SYN packet from 10.128.112.225 to 10.128.112.255. The packet details show the Ethernet II, Internet Protocol Version 4, and TCP fields. The packet bytes show the raw data in hexadecimal and ASCII.



**SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



Department of Computer Engineering
Class: S.Y. B.Tech.

Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

b. Port

Wireshark packet capture showing a TCP connection on port 57599. The capture shows a SYN exchange followed by several data segments. The packet list on the left shows packets 2 through 37. The packet details pane on the right shows the structure of a TCP segment, including the source and destination ports (57599). The packet bytes pane on the right shows the raw data of the selected packet.

c. Ack

Wireshark packet capture showing a TCP connection on port 57731. The capture shows a SYN exchange followed by several data segments. The packet list on the left shows packets 39731 through 39776. The packet details pane on the right shows the structure of a TCP segment, including the source and destination ports (57731). The packet bytes pane on the right shows the raw data of the selected packet.



**SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



Department of Computer Engineering
Class: S.Y. B.Tech. Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

d. Payload

Wireshark packet capture showing a TCP segment of a reassembled PDU. The packet list shows a sequence of TCP segments from 15199 to 15253. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

3. Arp:

Wireshark packet capture showing ARP requests and responses. The packet list shows a sequence of ARP packets from 496 to 1549. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and ARP layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.



**SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)



Department of Computer Engineering
Class: S.Y. B.Tech. Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

4. Udp:

Wireshark packet capture for UDP. The packet list shows a single packet (No. 26674) from 10.120.112.15 to 255.255.255. The packet details pane shows Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Data (83 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

5. Http:

Wireshark packet capture for HTTP. The packet list shows a single packet (No. 7) from 10.120.112.15 to 10.120.112.225. The packet details pane shows Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.



**SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING**
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

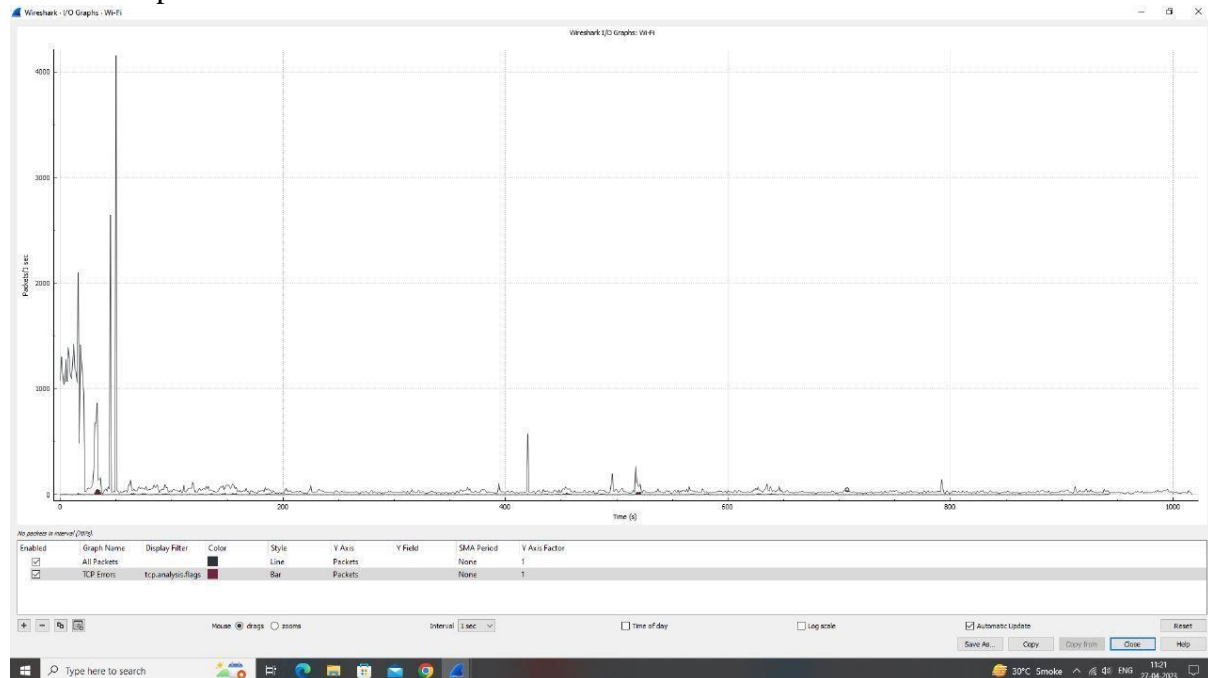


Department of Computer Engineering
Class: S.Y. B.Tech. Semester: IV

Course Code: DJ19CEL405

Course Name: Computer Networks Lab

6. I/O Graph:



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