Ex.No: 4	Installation of Wireshark, TCPdump and observe the data transferred in client-server communication using UDP/TCP and Identify the UDP/TCP datagram.

Aim:

To install wireshark, TCPdump and observe the data transferred in client-server communicationusing UDP/TCP and Identify the UDP/TCP datagram.

Wireshark:

Wireshark is an open-source tool for profiling network traffic and analyzing packets. Such tool isoften referred as a network analyzer, network protocol analyzer or sniffer.

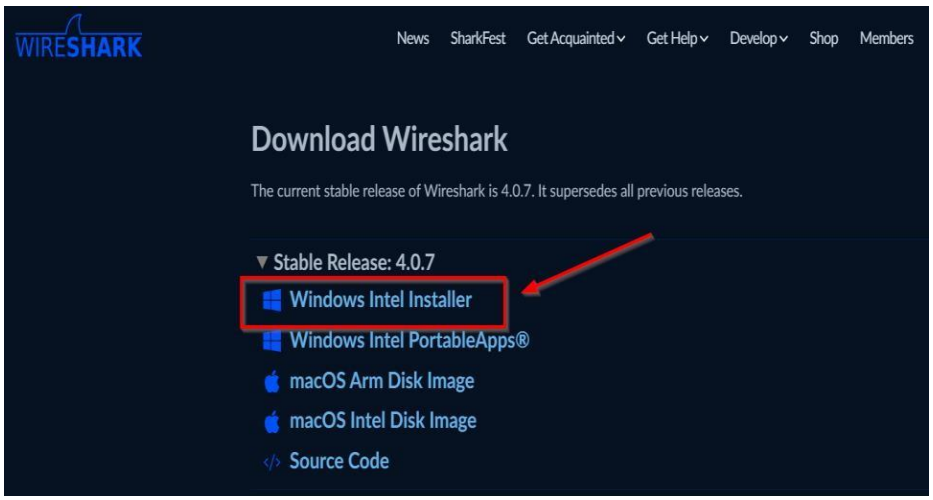
It is used to understand how communication takes place across a network and to analyze what wentwrong when an issue in communication arises.

It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and framerelay connections, among others, and stores that data for offline analysis.

Wireshark allows you to filter the log before the capture starts or during analysis, For example, you can set a filter to see TCP traffic between two IP addresses, or you can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it has become the standardtool for packet analysis.

Installation of Wireshark:

Step 1: Your first step is to head to the Wireshark download page **https://www.wireshark.org/download.html** and locate the Windows installer.



Step 2: You will be presented with the Wireshark wizard to guide you through the installation. Click "Next."

Step 3: Next, you can review, agree to the license agreement, and click "Noted" to continue.

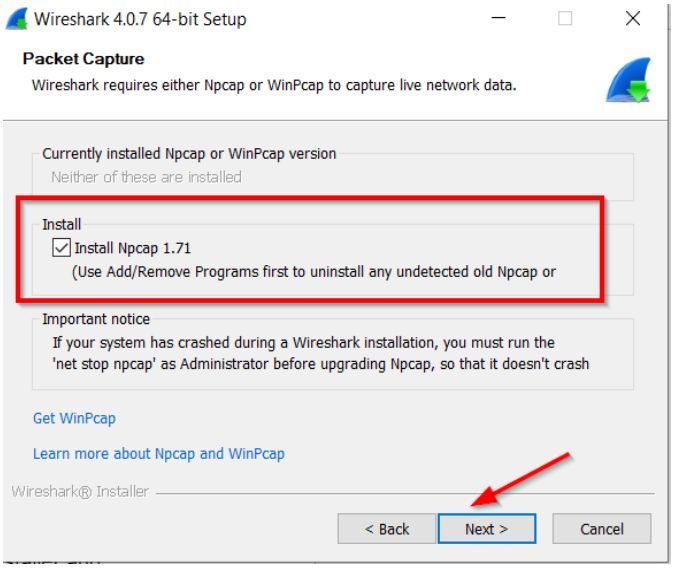
Step 4: You will be asked what components you want to install. You can make your

choice and thenclick “Next.”

Step 5: Choose a directory to install Wireshark in, showing you the space required to install it.

Step 6: Install **Ncap.**

Ncap is an open-source library for packet capture and network analysis which allows Wireshark to capture and analyze network traffic effectively. It enhances Wireshark's capabilities byproviding optimized packet capture.



Step 7: The next screen will ask if you want to install USBPcap, an open-source USB packet capture utility that lets you capture raw USB traffic, helping analyze and troubleshoot USB devices,this is not mandatory.

Click “Install” to begin the installation.

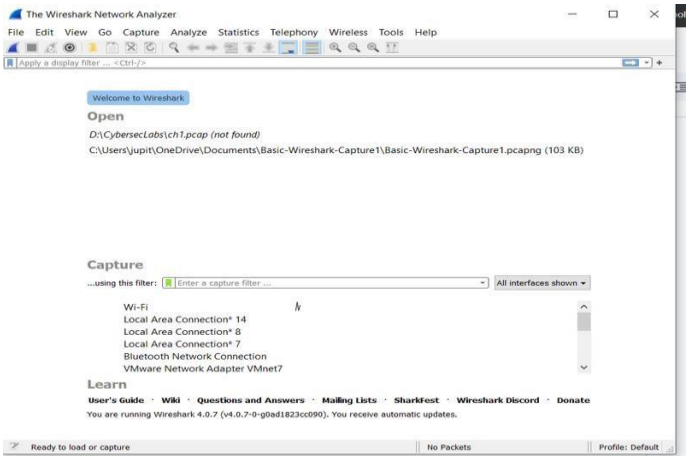
Step 8: Wireshark will now begin the installation process. A window will pop up duringinstallation to install cap.

Step 9: Ncap will begin the installation; click “Next” once complete.

Step 10: Wireshark will now complete its installation. Once complete, you can click “Next.”

Step 11: On the last window, click “Finish” to complete the setup**.**

Step 12: Wireshark will now be installed, and you can begin packet capturing.



When you install the wireshark program, the wireshark GUI with no data will be displayed.

Select one of the wireshark interface, eth0, eth1 will be displayed. Click “Start”for interface eth0to begin the Packet capture.

All packets being sent/received from/by the computer are now being captured by wireshark. Click”Start”.

Wireshark User Interface:

The wireshark interface has 5 major components;

- The **Command menus** are the standard pulldown menus located at top.
- The **Packet listing window** displays a one-line summary for each packet captured, it includes Packet number, Packet captured time, Packet’s source & destination address, Protocol type, Protocol specific information.
- The **Packet header details** window provides about packet selected in the packet listing window. It includes details about Ethernet frame and IP datagram of the packet. If the packet has been carried over by TCP/UDP, that details will also be displayed.
- **Packet contents window** display entire contents of the captured frame in both ASCII and hexadecimal format.
- In the **Packet display filter field,** the protocol name or other information can be entered to filter the information displayed in packet listing window.

Capturing Packets:

After installing and downloading wireshark, Launch it and click the name of an interface underInyerface List to start capturing packets.

Test Run:

Start any browser→ Start the wireshark software → Select an interface → Stop wireshark packetcapture once the browser has been displayed.

Colour coding: Packets will be highlighted in blue, green, black which helps to identify thetypes of traffic.

Green→ TCP traffic, Dark Blue → DNS traffic, Light Blue → UDP traffic, Black → TCPpackets with problems.

Inspecting Packets:

Click on any packet and go to the bottom pane.

Inspecting Packet flow:

We have a live packet data that contains all protocol message exchanged between yourcomputer and other network entities.

To filter the connection and to get a clear data type "http" in the filtering field. Note that directly typing the destination will not work as wireshark doesn't have ability to discern the protocolsfield.

To get more precise data set

http.host==www.netwoksecurity.eduRight click on any

packet → Select "Follow UDP Stream".

Close the window, change filter back to

"http.host==www.networksecurity.edu" follow apacket from the list that matches the filter.Use "Contains with other protocols."

TCPdump:

TCP (Transmission Control Protocol) facilitates the transmission of packets from source todestination.

Tcpdump is a command line utility that allows you to capture and analyze network traffic goingthrough your system. It is often used to help troubleshoot network issues, as well as a security tool.

It is a network monitoring and management utility that captures and records TCP/IP data on the run time. Tcpdump is designed to provide statistics about the number of packets received and captured at the operating node for network performance analysis, debugging and diagnosing networkbottlenecks and other network-oriented tasks.

Identifying UDP/TCP datagram:

IP packets have 8-bit header (Protocol for v4 and Next Header in v6) which determines which transport-layer protocol is used in the payload. For example, if it's 6, the payload is a TCP segment,and if it's 17 then that is an UDP.

TCP is connection-oriented while UDP is connectionless.

TCP sends data in a particular sequence, whereas there is no fixed order for UDP protocol.

Result:

Thus, the installation of Wireshark, TCPdump and observing the data transferred in client-servercommunication using UDP/TCP and Identifying the UDP/TCP datagram has been executed successfully.