PART A

(PART A: TO BE COMPLETED BY STUDENTS)

Experiment No.4

A.1 Aim:

Use Wire shark to understand the operation of TCP/IP layers:

A.2 Prerequisite:

Knowledge of OSI and TCP/IP model.

A.3 Objective:

Demonstration, identification and analysis of different types of protocols used and packets transmitted in TCP/IP by using Wireshark.

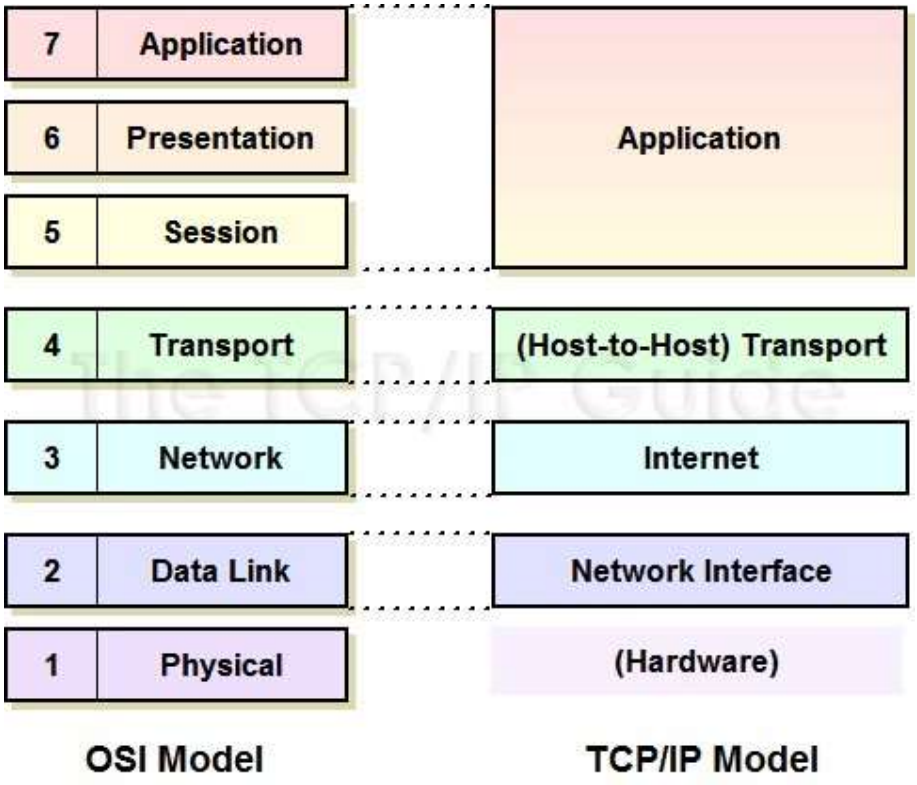
A.4 Outcome:

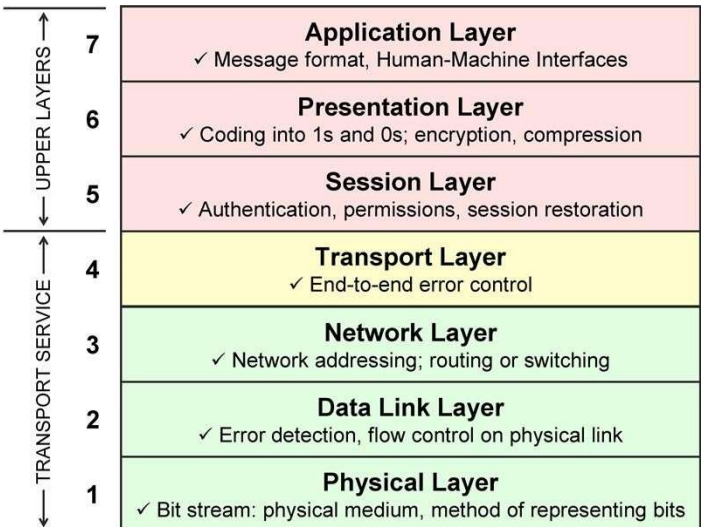
After successful completion of this experiment students will be able to

- Demonstration of a network packet analyzer and presentation of captured packet data in as much detail as possible.
- Ability to use network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

A.5 Theory:

OSI MODEL & TCP/IP MODEL


7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data Link
1
Physical
Application
(Host-to-Host) Transport
Internet
Network Interface
(Hardware)
OSI Model
TCP/IP Model


UPPER LAYERS
TRANSPORT SERVICE
7
Application Layer
✓ Message format, Human-Machine Interfaces
6
Presentation Layer
✓ Coding into 1s and 0s; encryption, compression
5
Session Layer
✓ Authentication, permissions, session restoration
4
Transport Layer
✓ End-to-end error control
3
Network Layer
✓ Network addressing; routing or switching
2
Data Link Layer
✓ Error detection, flow control on physical link
1
Physical Layer
✓ Bit stream: physical medium, method of representing bits

	OSI Layer	TCP/IP	Datagrams are called
Software	**Layer 7** Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	Upper Layer Data
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	**Segment**
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	**Packet**
Hardware	**Layer 2** Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	**Frame**
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	**Bits**

1.1. What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

1.1.1. Some intended purposes

Here are some reasons people use Wireshark:

- Network administrators use it to *troubleshoot network problems*
- Network security engineers use it to *examine security problems*
- QA engineers use it to *verify network applications*
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals Wireshark can also be helpful in many other situations.

1.1.2. Features

The following are some of the many features Wireshark provides:

- Available for *UNIX* and *Windows*.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with *very detailed protocol information*.

- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- *Filter packets* on many criteria.
- *Search* for packets on many criteria.
- *Colorize* packet display based on filters.
- Create various *statistics*. • …and *a lot more!*

However, to really appreciate its power you have to start using it.

Figure 1.1, “Wireshark captures packets and lets you examine their contents.” shows Wireshark having captured some packets and waiting for you to examine them.

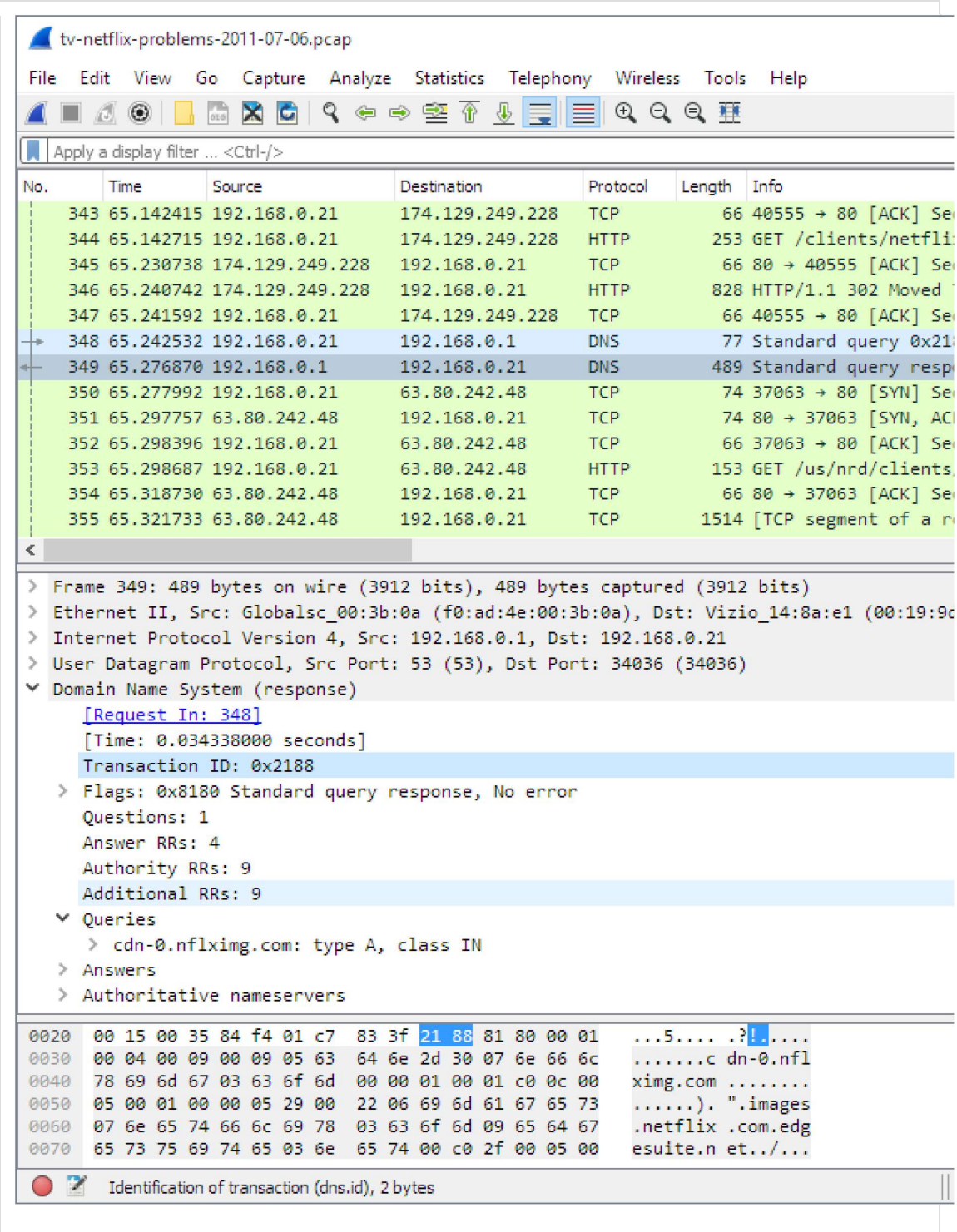


Figure 1.1. Wireshark captures packets and lets you examine their contents.

1.1.3. Live capture from many different network media

Wireshark can capture traffic from many different network media types, including Ethernet, Wireless LAN, Bluetooth, USB, and more. The specific media types supported may be limited by several factors, including your hardware and operating system. An overview of the supported media types can be found at https://wiki.wireshark.org/CaptureSetup/NetworkMedia.

1.1.4. Import files from many other capture programs

Wireshark can open packet captures from a large number of capture programs.

1.1.5. Export files for many other capture programs

Wireshark can save captured packets in many formats, including those used by other capture programs.

1.1.6. Many protocol dissectors

There are protocol dissectors (or decoders, as they are known in other products) for a great many protocols.

1.1.7. Open Source Software

Wireshark is an open source software project, and is released under the GNU General Public License (GPL). You can freely use Wireshark on any number of computers you like, without worrying about license keys or fees or such. In addition, all source code is freely available under the GPL. Because of that, it is very easy for people to add new protocols to Wireshark, either as plugins, or built into the source, and they often do!

1.1.8. What Wireshark is not

Here are some things Wireshark does not provide:

- Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
- Wireshark will not manipulate things on the network, it will only "measure" things from it. Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).

Refer:

1. https://www.wireshark.org/docs/wsug_html_chunked/ChCustCommandLine.html
2. https://www.javatpoint.com/wireshark
3. (https://www.youtube.com/watch?v=TkCSr30UojM)

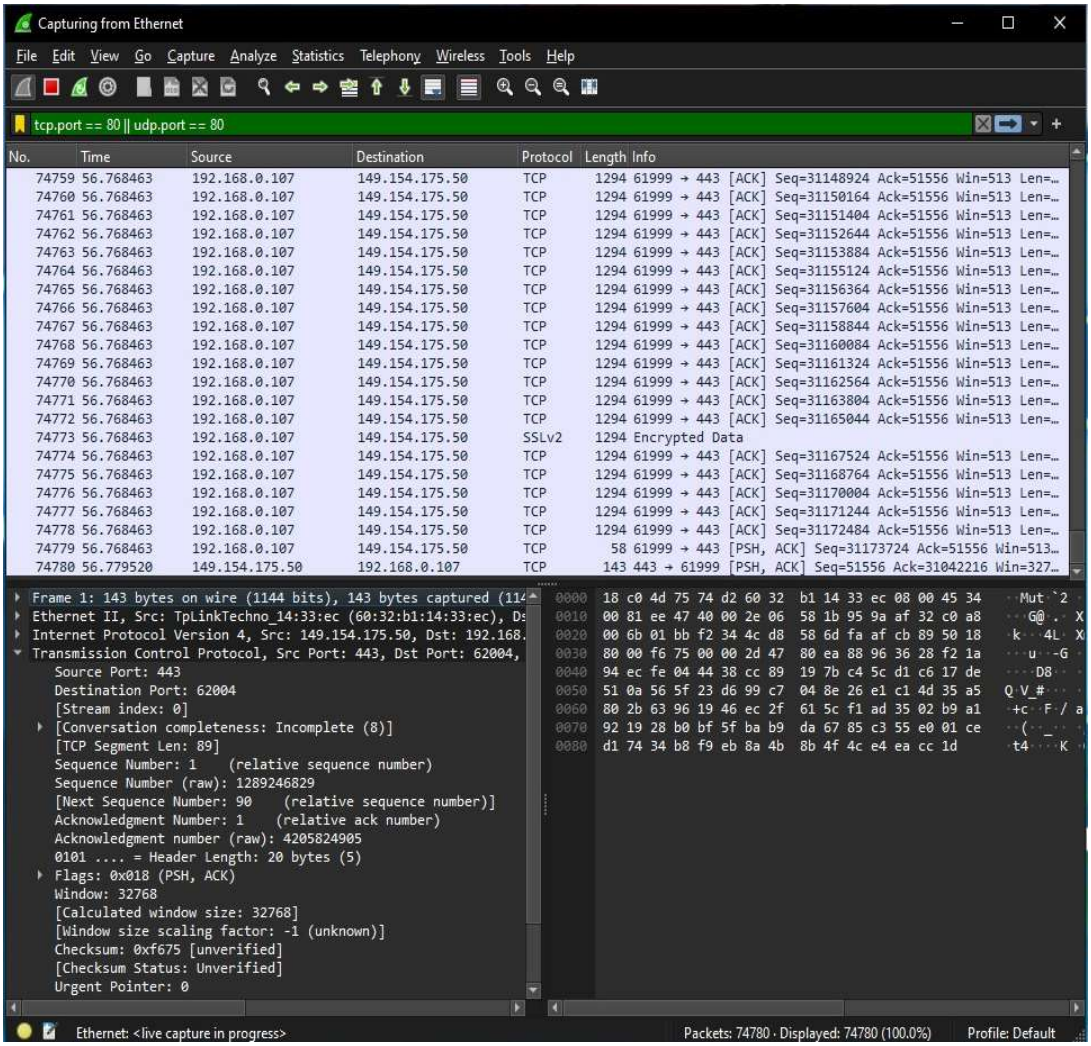
PART B

(PART B : TO BE COMPLETED BY STUDENTS)

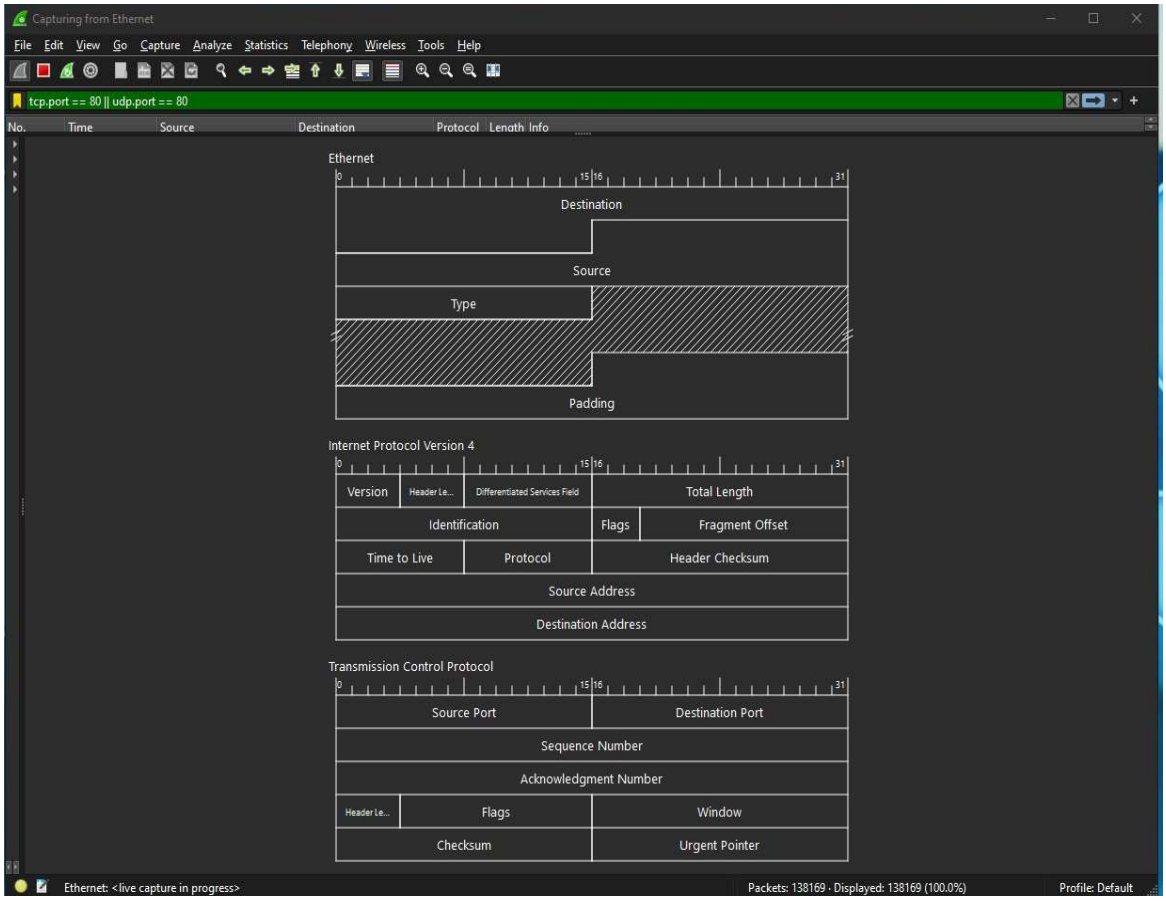
Roll No. A11	Name: Khan Mohammad TAQI
Class : TE-A	Batch : A1
Date of Experiment:	Date of Submission
Grade :	

B.1 Document created by the student:

Packets transmitted in TCP/IP by using Wireshark



Packet Diagram



B.3 Observations and learning:

Wireshark is a powerful network protocol analyzer that enables users to capture, analyze, and understand network traffic in real time. By examining packets and protocols, users can gain valuable insights into network communication, troubleshooting, and security.

B.4 Conclusion:

Successfully learned how to use Wireshark to analyze network traffic. I captured and examined packets to understand network protocols, data transmission, and troubleshooting techniques. This hands-on experience was really helpful in understanding how networks work.

B.5 Question of Curiosity

Q1: Briefly explain why there are two layered protocols in networking, TCP/IP four layered and OSI seven layered?

The TCP/IP and OSI models were developed to provide a standardized framework for network communication, each serving different purposes and perspectives in networking.

TCP/IP Four-Layer Model

The TCP/IP model was created by the Defense Advanced Research Projects Agency (DARPA) and is designed to ensure interoperability between different types of hardware and software. It has four layers:

1. Link Layer: Handles the physical connection between devices.

2. Internet Layer: Manages packet routing through the network.

3. Transport Layer: Ensures reliable data transfer with protocols like TCP and UDP.

4. Application Layer: Supports network applications and end-user processes.

OSI Seven-Layer Model

The OSI (Open Systems Interconnection) model, developed by the International Organization for Standardization (ISO), provides a more detailed and abstract framework:

1. Physical Layer: Manages the physical medium for data transmission.

2. Data Link Layer: Ensures reliable node-to-node data transfer.

3. Network Layer: Handles routing and forwarding of data.

4. Transport Layer: Manages end-to-end communication and error recovery.

5. Session Layer: Controls dialogues (connections) between computers.

6. Presentation Layer: Translates data between the application and the network.

7. Application Layer: Interfaces directly with user applications.

Comparison and Purpose

- TCP/IP Model: More practical and closely aligned with real-world protocols, focusing on the primary functions needed for network communication.

- OSI Model: More theoretical and comprehensive, breaking down network interactions into finer-grained layers to facilitate understanding, troubleshooting, and protocol development.

Q2: What is Wireshark? Mention the Uses of Wireshark.

Wireshark is a powerful, open-source network protocol analyzer used for capturing and inspecting the data traveling across a network in real time. It allows users to see what is happening on their network at a microscopic level, making it a valuable tool for network administrators, security analysts, and developers.

Uses of Wireshark

1.Network Troubleshooting: Identify and resolve network issues such as slow performance, connectivity problems, and packet loss.

2. Security Analysis: Detect and investigate network security threats, intrusions, and vulnerabilities.

3. Protocol Development: Analyze and debug new network protocols during development.

4. Network Performance Monitoring: Monitor network traffic to ensure efficient and optimal performance.

5. Educational Purposes: Teach and learn about network protocols, data structures, and networking concepts.

Q 3: a. Which Layer of the TCP/IP 4 layer model this address belong to.

In the TCP/IP four-layer model, network addresses belong to specific layers depending on the type of address:

1. Link Layer:

MAC Address: Media Access Control (MAC) addresses are hardware addresses assigned to network interfaces for communication on the physical network segment.

2. Internet Layer:

IP Address: Internet Protocol (IP) addresses (IPv4 or IPv6) are used to identify devices on different networks and to route packets between them.

3. Transport Layer:

Port Number: Port numbers are used by the transport layer protocols (such as TCP and UDP) to identify specific processes or services on a host.

4. Application Layer:

Domain Name: Domain names (e.g., www.example.com) are used to identify resources on the network in a human-readable format and are resolved to IP addresses by the DNS (Domain Name System).

b. State the protocol appropriate to this address and any special characteristics for this address within the appropriate protocol.

The addresses are

i) 136.206.1.4
ii) 192.168.1.10
iii) 127.0.0.1
iv) 0C: 5F : 56 : C0 : DD: 08

v) Port 80

vi) Port 2000

i) 136.206.1.4

- Protocol: Internet Protocol (IP) - Characteristics:

- This is a public IPv4 address, indicating it is routable on the internet.

- Used for identifying a device on the global internet.

ii) 192.168.1.10

- Protocol: Internet Protocol (IP)

- Characteristics:

- This is a private IPv4 address, part of the 192.168.0.0/16 range.

- Commonly used in local area networks (LANs) and not routable on the public internet.

iii) 127.0.0.1

- Protocol: Internet Protocol (IP)

- Characteristics:

- This is a loopback address in IPv4.

- Used to refer to the local host or the device itself.

- Useful for testing and network diagnostics.

iv) 0C:5F:56:C0:DD:08

- Protocol: Media Access Control (MAC) - Characteristics:

- This is a MAC address.

- Unique identifier assigned to a network interface card (NIC) for communication on the physical network segment.

- Used at the Link Layer of the TCP/IP model.

v) Port 80

- Protocol: Transmission Control Protocol (TCP) - Characteristics:

- Default port for HTTP (Hypertext Transfer Protocol).

- Used for unencrypted web traffic.

vi) Port 2000

- Protocol: Transmission Control Protocol (TCP) / User Datagram Protocol (UDP)

- Characteristics:

- Often used for Cisco SCCP (Skinny Call Control Protocol) in VoIP.

- Can be used by various applications; not assigned to a single well-known service.

Each address serves specific purposes within their respective protocols, facilitating the proper routing, identification, and communication of data across networks.

Q4: PORT Nos belong to which layer?

Port numbers belong to the **Transport Layer** of the TCP/IP model. The Transport Layer is responsible for end-to-end communication and data transfer management between devices on a network. Port numbers are used by transport layer protocols, such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), to identify specific processes or services on a host, enabling the correct application to receive the data.

Q5: What is a packet? In which layer it is created?
A packet is a formatted unit of data carried by a network. It is the fundamental unit of communication over a network, consisting of both control information and user data.

Creation of a Packet

Packets are created at the **Internet Layer** of the TCP/IP model.

Details of a Packet

- **Control Information:** Includes headers and metadata such as source and destination IP addresses, error detection codes, sequencing information, and other details required for routing and delivering the packet.

- **User Data**: The actual data being transmitted, which can include parts of files, messages, or other types of user information.

When data is transmitted over a network, it is encapsulated into packets at the Internet Layer, where IP addressing and routing information are added. This process ensures that the data can be correctly routed across different networks to its destination.

Q6: What is color coding in Wireshark?
Color coding in Wireshark is a feature that visually distinguishes different types of network traffic to help users quickly identify and analyze packets based on their protocols and other characteristics. This visual aid enhances readability and makes it easier to spot unusual or suspicious traffic patterns.

Key Aspects of Color Coding in Wireshark

- Default Coloring Rules: Wireshark comes with a set of default coloring rules that apply colors to packets based on common protocols and packet types.

- TCP Traffic: Typically shown in light blue for established connections.

- UDP Traffic: Often displayed in light purple.

- HTTP Traffic: Usually highlighted in green.

- DNS Traffic: Often shown in light blue.

- Errors: Problematic packets, such as those with malformed data, might be shown in red.

- Custom Coloring Rules: Users can create custom coloring rules to highlight specific traffic or conditions that are of interest to them. This can be based on any packet field or protocol.

- Enhanced Analysis: The color coding helps users quickly identify different types of traffic, making it easier to focus on particular packets, analyze network behavior, and troubleshoot issues.

By using color coding, Wireshark enhances the efficiency and effectiveness of network analysis and troubleshooting.

Q7: Write the features of Wireshark?
Features of Wireshark

-Real-Time Packet Capture: Captures network packets in real time from various network interfaces, allowing for live analysis.

-Deep Packet Inspection: Provides detailed information about each packet, including protocol-specific data, headers, and payloads.

-Protocol Decoding: Supports a wide range of network protocols and can decode them for detailed analysis. This includes both common and less frequently used protocols.

-Filtering and Search: Offers powerful filtering capabilities using display filters and capture filters to narrow down the packets of interest. Advanced search options help locate specific packets or data patterns.

-Color Coding: Uses color coding to differentiate packet types and protocols visually, making it easier to identify and analyze specific traffic.

Q8: Write the filters used in Wireshark?
In Wireshark, filters help narrow down network traffic for analysis:

-Capture Filters: Set before capturing data to specify which packets to capture.

Example: tcp port 80 (captures only TCP traffic on port 80).

-Display Filters: Refine and analyze captured packets based on criteria.

Example: ip.addr == 192.168.1.1 (displays packets with a specific IP address).

-Protocol-Specific Filters: Focus on packets from specific protocols.

Example: dns (filters DNS packets).

-Advanced Filters: Combine expressions for more precise filtering.

Example: ip.src == 192.168.1.1 && tcp.dstport == 443 (displays packets from a specific IP with a destination port of 443).

These filters assist in isolating and analyzing specific network traffic.

Q9: What is packet sniffing?

Packet sniffing is the process of intercepting and analyzing network packets as they travel across a network. This technique allows users to capture and examine the data, including headers and payloads, to monitor network performance, troubleshoot issues, and detect security threats. Tools like Wireshark and tcpdump are commonly used for packet sniffing, providing valuable insights into network behavior and protocol interactions.