



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

Experiment No. 5

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

- Ethernet Layer: Frame header, Frame size etc.
- Data Link Layer: MAC address, ARP (IP and MAC address binding)
- Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo)
- Transport Layer: TCP Ports, TCP handshake segments etc.
- Application Layer: DHCP, FTP, HTTP header formats

Resource required: Computer or Laptop, Wireshark Installed, Access to a local network where you can capture packets

Theory:

Wireshark : it's a secret agent used to spy, understanding the things working behind used by hacker and new learner used to checks how internet works

It's a detective tool for computer networks- to check what is happening in the network troubleshoot issues or to check how the network protocols work. whether data is traveling from any ethernet, Bluetooth, wifi or any networks

Networking protocols:

Networking protocols are formal rules and conventions that govern how data is transmitted and received across networks. They ensure that devices can communicate effectively, securely, and reliably.

② 1. Communication Protocols

These define how data is transferred between devices.

Protocol	Description
TCP (Transmission Protocol)	Control Connection-oriented; ensures reliable data transfer.



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

Protocol	Description
UDP (User Datagram Protocol)	Connectionless; faster but less reliable than TCP.
IP (Internet Protocol)	Routes packets between devices across networks (IP addresses).
ICMP (Internet Control Message Protocol)	Sends error messages (e.g., "host unreachable", "ping").

🌐 2. Internet & Web Protocols

Protocol	Description
HTTP (Hypertext Transfer Protocol)	Used for web communication (insecure).
HTTPS (HTTP Secure)	Secure version of HTTP using SSL/TLS.
FTP (File Transfer Protocol)	Transfers files between systems (can be insecure).
SFTP (SSH File Transfer Protocol)	Secure file transfer over SSH.
DNS (Domain Name System)	Resolves domain names to IP addresses.

🔧 3. Network Management Protocols

Protocol	Description
DHCP (Dynamic Host Configuration Protocol)	Automatically assigns IP addresses to devices.
SNMP (Simple Network Management Protocol)	Monitors and manages network devices.
NTP (Network Time Protocol)	Synchronizes time across devices.



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

4. Security Protocols

Protocol	Description
SSL/TLS (Secure Sockets Layer / Transport Layer Security)	/ Encrypts data over a network (used in HTTPS, email, etc.).

SSH (Secure Shell)	Secure remote login and command execution.
--------------------	--

5. Routing Protocols

Protocol	Description
RIP (Routing Information Protocol)	Basic distance-vector routing protocol.
OSPF (Open Shortest Path First)	Link-state routing; more efficient than RIP.
BGP (Border Gateway Protocol)	Core routing protocol of the internet.

Common Protocol Stack Example (TCP/IP Model):

Layer	Example Protocols
-------	-------------------

Application HTTP, FTP, DNS, SMTP

Transport TCP, UDP

Internet IP, ICMP

Link Ethernet, Wi-Fi

Practical: Using Wireshark to Understand TCP/IP Layers

Preparation:

- Install Wireshark on your PC/laptop.
- Connect to an active network (LAN or Wi-Fi).
- Make sure you have permission to capture network traffic on this network.



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

The Ethernet layer is part of the Data Link Layer (Layer 2) of the OSI model. It defines how data is formatted into frames, how devices are addressed (using MAC addresses), and how error detection is performed for communication within a Local Area Network (LAN).

Ethernet is the most widely used LAN technology today.

❖ Functions of Ethernet Layer

1. Framing

- Breaks network-layer packets into manageable units called Ethernet frames.
- Adds headers (source MAC, destination MAC) and trailers (CRC error checking).

2. Addressing

- Uses MAC (Media Access Control) addresses to identify devices on a LAN.
- Example: 00:1A:2B:3C:4D:5E.

3. Error Detection

- Uses CRC (Cyclic Redundancy Check) in the frame trailer to detect errors.

4. Access Control

- Uses CSMA/CD (Carrier Sense Multiple Access with Collision Detection) in traditional Ethernet to handle multiple devices on the same medium.
- Modern Ethernet (switch-based) reduces collisions.

☒ How to Use Wireshark to Analyze the Ethernet Layer (Layer 2)

❖ Step 1: Capture Traffic

1. Open Wireshark.

2. Start capturing on the appropriate network interface (e.g., Wi-Fi or Ethernet).



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

3. Perform some network activity (like opening a website).
4. Stop the capture after collecting some packets.

❖ Step 2: Filter for Ethernet Packets

Ethernet is the base layer for most packets, so you don't need a specific filter to see them. But to narrow down:

- Use a filter like eth or just click on any packet.

❖ Step 3: Examine the Ethernet Frame

Click on a packet (e.g., an HTTP or TCP packet), and expand the first section labeled:

Frame X: <number of bytes on wire>, <number of bytes captured>

This tells you:

- Frame size on the wire (in bytes): The actual size as transmitted.
- Captured size: May be smaller if the capture was truncated.

Then expand the section:

Ethernet II

You'll see:

Field	Description
-------	-------------

Destination MAC address MAC address of the device the frame is being sent to

Source MAC address MAC address of the sender

Type Ethernet Type (e.g., 0x0800 for IPv4)

❖ Step 4: Important Ethernet Fields

Field	Purpose
-------	---------

Preamble (Not shown in Wireshark) 7-byte sync pattern + 1-byte Start Frame Delimiter (SFD)

Destination MAC Identifies the receiver



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

Field	Purpose
Source MAC	Identifies the sender
Type / Length	Indicates which protocol is encapsulated (IP, ARP, etc.)
Payload	The actual data (e.g., IP packet)
FCS (Frame Check Sequence)	Error detection (not usually captured by Wireshark)

Wireshark Screenshot:

Network Interface: eth

No.	Time	Source	Destination	Protocol	Length	Info
596	0.910270	57.144.125.32	192.168.2.138	TCP	60	443 → 36119 [ACK] Seq=99 Ack=91 Win=450 Len=0
597	0.919475	103.185.244.162	192.168.2.138	UDP	1274	443 → 61860 Len=1232
598	0.919597	103.185.244.162	192.168.2.138	UDP	1274	443 → 61860 Len=1232
599	0.919655	103.185.244.162	192.168.2.138	UDP	1274	443 → 61860 Len=1232
600	0.922645	103.185.244.162	192.168.2.138	UDP	1274	443 → 61860 Len=1232

Frame 596: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{774AE992-F6EB-42BE-B1DA-6FDAC46C4E13}
Section number: 1
Interface id: 0 (\Device\NPF_{774AE992-F6EB-42BE-B1DA-6FDAC46C4E13})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 17, 2025 16:27:41.672977000 India Standard Time
UTC Arrival Time: Sep 17, 2025 10:57:41.672977000 UTC
Epoch Arrival Time: 1758106661.672977000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.001089000 seconds]
[Time delta from previous displayed frame: 0.001089000 seconds]
[Time since reference or first frame: 0.910270000 seconds]
Frame Number: 596
Frame Length: 60 bytes (480 bits)
Capture Length: 60 bytes (480 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: MercuryCommu_28:d0:26 (38:6b:1c:28:d0:26), Dst: NaxiangTechn_e:fc:18 (ec:9a:0c:1e:fc:18)
> Destination: NaxiangTechn_e:fc:18 (ec:9a:0c:1e:fc:18)
> Source: MercuryCommu_28:d0:26 (38:6b:1c:28:d0:26)
Type: IPv4 (0x0800)
[Stream index: 0]
Padding: 000000000000
> Internet Protocol Version 4, Src: 57.144.125.32, Dst: 192.168.2.138
> Transmission Control Protocol, Src Port: 443, Dst Port: 36119, Seq: 99, Ack: 91, Len: 0



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	103.185.244.162	192.168.2.138	UDP	1274	443 + 61860 Len=1232
2	0.000000	103.185.244.162	192.168.2.138	UDP	1274	443 + 61860 Len=1232
3	0.000155	103.185.244.162	192.168.2.138	UDP	1274	443 + 61860 Len=1232
4	0.000201	103.185.244.162	192.168.2.138	UDP	1274	443 + 61860 Len=1232
5	0.000301	103.185.244.162	192.168.2.138	UDP	1274	443 + 61860 Len=1232

Frame 1: 1274 bytes on wire (10192 bits), 1274 bytes captured (10192 bits) on interface \Device\NPF_{774AE992-F6EB-42BE-B1DA-6FDAC46C4E13})

Section number: 1

> Interface id: 0 (\Device\NPF_{774AE992-F6EB-42BE-B1DA-6FDAC46C4E13})

Encapsulation type: Ethernet (1)

Arrival Time: Sep 17, 2025 16:27:40.762707000 India Standard Time

UTC Arrival Time: Sep 17, 2025 10:57:40.762707000 UTC

Epoch Arrival Time: 175810660.762707000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

Frame Length: 1274 bytes (10192 bits)

Capture Length: 1274 bytes (10192 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:udp:data]

[Coloring Rule Name: UDP]

[Coloring Rule String: udp]

> Ethernet II, Src: MercuryCommu_28:d0:26 (38:6:b1:c2:28:d0:26), Dst: MaxiangTechn_e:fc:18 (ec:9:a:0:8:0:18)

> Destination: MaxiangTechn_e:fc:18 (ec:9:a:0:c1e:f1:18)

> Source: MercuryCommu_28:d0:26 (38:6:b1:c2:28:d0:26)

Type: IPv4 (0x800)

[Stream index: 8]

> Internet Protocol Version 4, Src: 103.185.244.162, Dst: 192.168.2.138

User Datagram Protocol, Src Port: 443, Dst Port: 61860

Data (1232 bytes)

Step-by-Step Wireshark Analysis for Data Link Layer

1. Start a Packet Capture

1. Open Wireshark.
2. Choose the correct network interface (e.g., Ethernet, Wi-Fi).
3. Click Start Capture (the shark fin icon).
4. Perform some network activity (e.g., open a website or ping a local IP) to generate packets.

2. Data Link Layer – MAC Addresses

- The Data Link Layer is Layer 2 of the OSI model and is responsible for MAC addressing and frame delivery on a local network.

Wireshark is a packet analyzer that lets you capture and inspect frames traveling on a network.

At the Data Link Layer (Layer 2), you'll mostly be looking at Ethernet frames (on wired LANs) or 802.11 frames (on Wi-Fi).

In the Packet Details Pane, you'll see multiple expandable layers:

- Frame → Overall capture info (arrival time, interface).
- Ethernet II (Data Link Layer) → Contains MAC addresses and EtherType.



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

- Internet Protocol (IP) → Network layer info.
- TCP/UDP → Transport layer info.

⌚ Filter to See MAC Address Information

Use this filter:

eth

⌚ How to View MAC Addresses:

1. Click on a packet in the capture (e.g., an ARP or IP packet).
2. Expand the Ethernet II section.
3. You will see:
 - Source: MAC address of the sender.
 - Destination: MAC address of the receiver.
 - Example:
 - Ethernet II
 - Destination: 00:1a:2b:3c:4d:5e
 - Source: 5e:4d:3c:2b:1a:00
 - Type: IPv4 (0x0800)

```
C:\Users\janu>ping www.youtube.com
```

```
Pinging youtube-ui.l.google.com [142.250.70.110] with 32 bytes of data:  
Reply from 142.250.70.110: bytes=32 time=14ms TTL=116  
Reply from 142.250.70.110: bytes=32 time=17ms TTL=116  
Reply from 142.250.70.110: bytes=32 time=17ms TTL=116  
Reply from 142.250.70.110: bytes=32 time=14ms TTL=116
```

```
Ping statistics for 142.250.70.110:
```

```
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
  Approximate round trip times in milli-seconds:  
    Minimum = 14ms, Maximum = 17ms, Average = 15ms
```



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2409:40c2:2042:4122..	2620:1ec:bdff:58	TCP	75	45075 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
2	0.046240	2620:1ec:bdff:58	2409:40c2:2042:4122..	TCP	86	443 → 45075 [ACK] Seq=1 Ack=2 Win=83 Len=0 SRE=2
3	0.114613	2409:40c2:2042:4122..	64:ffffb9:3489:6ad9	TLSv1.2	332	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4	0.171854	2620:1ec:bdff:68	2409:40c2:2042:4122..	TLSv1.2	113	Application Data
5	0.173850	2620:1ec:bdff:68	2409:40c2:2042:4122..	TLSv1.2	98	Application Data
6	0.173850	2620:1ec:bdff:68	2409:40c2:2042:4122..	TCP	74	443 → 45103 [FIN, ACK] Seq=64 Ack=1 Win=83 Len=0
7	0.173936	2409:40c2:2042:4122..	2620:1ec:bdff:68	TCP	74	45103 → 443 [ACK] Seq=1 Ack=65 Win=255 Len=0
8	0.174398	2409:40c2:2042:4122..	2620:1ec:bdff:68	TCP	74	45103 → 443 [FIN, ACK] Seq=1 Ack=65 Win=255 Len=0
9	0.224364	2620:1ec:bdff:68	2409:40c2:2042:4122..	TCP	74	443 → 45103 [ACK] Seq=65 Ack=2 Win=83 Len=0
10	0.224364	2620:1ec:bdff:68	2409:40c2:2042:4122..	TCP	74	[TCP Dup ACK 98] 443 → 45103 [ACK] Seq=65 Ack=2 Win=83 Len=0

⌚ 3. ARP – IP to MAC Binding

ARP (Address Resolution Protocol) maps an IP address to a MAC address within a local network.

⌚ Filter ARP Packets:

Use this filter:

arp

⌚ What You'll See:

- Who has 192.168.1.1? Tell 192.168.1.2
 - This is a request from one host asking for the MAC address associated with an IP.
- 192.168.1.1 is at 00:1a:2b:3c:4d:5e
 - This is the reply showing the IP-to-MAC mapping.

⌚ Expand the ARP Section

In an ARP packet:

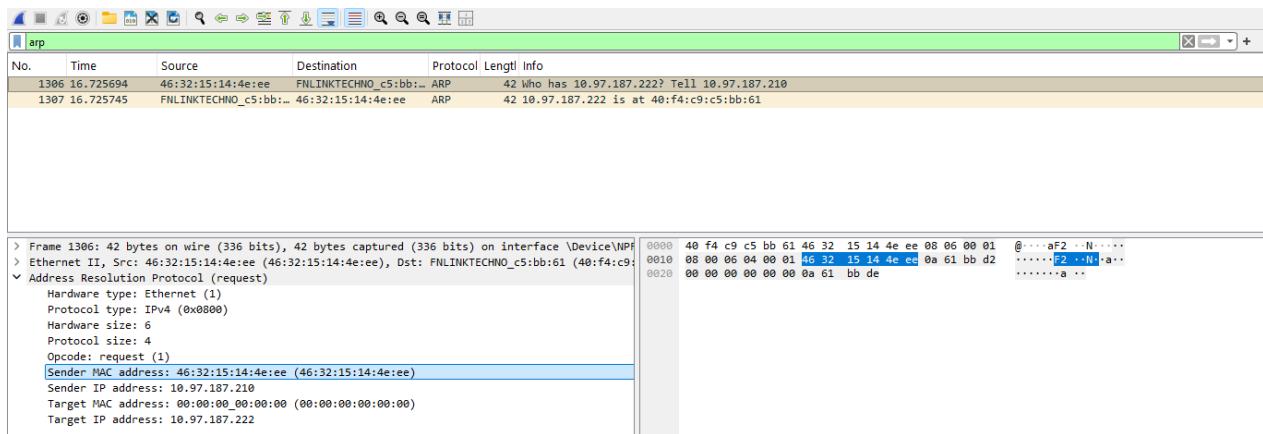
- Sender MAC address
- Sender IP address
- Target MAC address
- Target IP address



Shri Yashwantrao Bhonsale Education Society's
YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY
(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

This allows you to clearly see the binding between IP and MAC addresses.



🌐 NETWORK LAYER (Layer 3)

At the Network Layer, the main components you're going to observe are:

- IP Packets (IPv4 or IPv6)
- Fragmentation
- ICMP (Internet Control Message Protocol) — for diagnostics like ping/traceroute

Let's go step-by-step:

▀ 1. IP Packets – Header and Fragmentation

⌚ Filter:

ip

⌚ How to View IP Header:

1. Select an IP packet in your capture (e.g., HTTP, ICMP, or any IP-based traffic).
2. Expand the Internet Protocol Version 4 (IPv4) section.

You'll see fields like:

- Version (4 for IPv4)
- Header Length
- Total Length (size of the packet including header and data)
- Identification (used in fragmentation)



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

- Flags (DF – Don't Fragment, MF – More Fragments)
- Fragment Offset (position of this fragment in the original datagram)
- Time To Live (TTL)
- Protocol (e.g., 1 = ICMP, 6 = TCP, 17 = UDP)
- Source IP
- Destination IP

http											
No.	Time	Source	Destination	Protocol	Length	Info					
755	6.024104	4.240.189.64	10.97.187.222	TCP	1334	80 → 45109 [ACK] Seq=648961 Ack=1 Win=21 Len=1280					
+ 1148	13.224955	10.97.187.222	4.240.189.64	HTTP	397	GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.19127.20240/i640.c2rx?cacheHostOrigin=b.c2r.ts.cdn...					
1189	13.444624	2409:40c2:2042:412...:684	2a04:4e42:9::684	HTTP	255	HEAD /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.19127.20240/i640.cab HTTP/1.1					
1225	13.635369	2a04:4e42:9::684	2409:40c2:2042:412...:684	HTTP	702	HTTP/1.1 200 OK					
1226	13.651388	2409:40c2:2042:412...:684	2a04:4e42:9::684	HTTP	255	HEAD /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.19127.20240/i640.cab HTTP/1.1					
1237	13.852870	2a04:4e42:9::684	2409:40c2:2042:412...:684	HTTP	702	HTTP/1.1 200 OK					
1375	17.415451	10.97.187.222	4.240.189.64	HTTP	351	GET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Office/Data/16.0.19127.20240/i640.cab.php?cacheHostOrigin=officecdn...					
+ 2085	28.101517	4.240.189.64	10.97.187.222	HTTP	960	HTTP/1.1 200 Partial Content					

> Frame 1148: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface \Device\NPF_{...}	F2:N@...-a-E-
> Ethernet II, Src: FNLINKTECHNO_5:bb:61 (40:f4:c9:c5:bb:61), Dst: 46:32:15:14:e:ee (46:32:15:14:e:ee)	...:00..U:a...
Internet Protocol Version 4, Src: 10.97.187.222, Dst: 4.240.189.64	@:P:j..TtBq...
0100 = Version: 4*2...!
0101 = Header Length: 20 bytes (5)	
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)	
Total Length: 383	
Identification: 0x1b51 (6993)	
> 010. = Flags: 0x2, Don't fragment	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 128	
Protocol: TCP (6)	
Header Checksum: 0x55b8 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 10.97.187.222	
Destination Address: 4.240.189.64	
[Stream index: 1]	
> Transmission Control Protocol, Src Port: 45115, Dst Port: 80, Seq: 1, Ack: 1, Len: 331	
> Hypertext Transfer Protocol	

0000 46 32 15 14 4e ee 40 f4 c9 c5 bb 61 08 00 45 00	F2:N@...-a-E-
0010 01 7f 1b 51 40 00 80 06 55 b8 0a 61 bd 0e 04 f0	...:00..U:a...
0020 bd 40 b0 3b 00 50 b5 6a ba e5 54 74 42 71 80 18	@:P:j..TtBq...
0030 00 0a f2 fe 00 00 01 01 08 02 32 5f c6 10 21*2...!
0040 28 6d 47 45 54 20 DF 70 72 2f 34 39 32 33 35 36	(mGET /pr/492350f6-3a01-4f97-b9c0-c7c6ddf67d60/Offic...
.... 0101 = Header Length: 20 bytes (5)	f6-3a01-4f97-b9c...
Total Length: 383	0-c7c6dd...
Identification: 0x1b51 (6993)	f67d60/0
> 010. = Flags: 0x2, Don't fragment	
...0 0000 0000 0000 = Fragment Offset: 0	
Time to Live: 128	
Protocol: TCP (6)	
Header Checksum: 0x55b8 [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 10.97.187.222	
Destination Address: 4.240.189.64	
[Stream index: 1]	
> Transmission Control Protocol, Src Port: 45115, Dst Port: 80, Seq: 1, Ack: 1, Len: 331	
> Hypertext Transfer Protocol	

2. ICMP – Internet Control Message Protocol

ICMP is used for:

- Echo Request/Reply (ping)
- Destination unreachable
- Time exceeded (traceroute)

Filter ICMP Traffic:

icmp

How to Generate ICMP:

- Open Terminal/Command Prompt and type:

ping 8.8.8.8



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

This generates ICMP Echo Requests and receives Echo Replies.

⌚ View ICMP Fields in Wireshark:

1. Select an ICMP packet.
2. Expand Internet Control Message Protocol section.

You'll see:

- Type:
 - 8 = Echo Request
 - 0 = Echo Reply
 - 3 = Destination Unreachable
 - 11 = Time Exceeded (TTL expired)
- Code (refines the message type)
- Checksum
- Identifier and Sequence Number (match requests to replies)

```
C:\Users\janu>ping 8.8.8.8
```

```
Pinging 8.8.8.8 with 32 bytes of data:
```

```
Reply from 8.8.8.8: bytes=32 time=58ms TTL=111
```

```
Reply from 8.8.8.8: bytes=32 time=44ms TTL=111
```

```
Reply from 8.8.8.8: bytes=32 time=47ms TTL=111
```

```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=111
```

```
Ping statistics for 8.8.8.8:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 44ms, Maximum = 58ms, Average = 49ms
```



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

The screenshot shows a Wireshark capture titled "icmp". The left pane displays a list of 10 captured frames, mostly ICMP Echo requests and replies between two hosts. The right pane shows the details of frame 884, which is an ICMP Echo request. The hex dump shows the raw bytes of the packet, and the ASCII dump shows the readable text "F2 N @ a E< u M v abcdefghijklmnopqrstuvwxyz wabcdefg hi".

No.	Time	Source	Destination	Protocol	Length	Info
884	8.2380236	10.97.187.222	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 884)
901	8.288826	8.8.8.8	10.97.187.222	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=111 (request in 884)
975	9.246153	10.97.187.222	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 976)
976	9.290452	8.8.8.8	10.97.187.222	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=111 (request in 975)
981	10.289514	10.97.187.222	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 991)
991	10.336268	8.8.8.8	10.97.187.222	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=111 (request in 981)
1008	11.314623	10.97.187.222	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 1009)
1009	11.365086	8.8.8.8	10.97.187.222	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=111 (request in 1008)

⌚ Goal:

Analyze TCP communication by capturing and interpreting:

- TCP Handshake (3-way handshake)
- TCP Source/Destination Ports
- TCP Segments (including flags, sequence numbers, etc.)

✍ Step-by-Step Process

Step 1: Start Wireshark and Begin Capture

1. Launch Wireshark.
2. Select your active network interface (usually Ethernet or Wi-Fi).
3. Click the blue shark fin button to start capturing.

Step 2: Generate TCP Traffic

You can open a web browser and go to a website (e.g., <http://example.com>) or use:
ping google.com

Or better:

telnet google.com 80

If Telnet is not installed:

curl <http://example.com>



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

This generates visible TCP traffic, including handshakes.

⌚ Step 3: Filter TCP Packets

In Wireshark's top filter bar, enter:

tcp

Press Enter. This filters only TCP traffic.

⌚ Step 4: Identify the TCP 3-Way Handshake

Look for 3 sequential packets between the same source and destination IP:

Example:

1. SYN — Initiates the connection
2. SYN, ACK — Acknowledges and responds
3. ACK — Final acknowledgment

Each packet will show flags:

No Source Destination Info

- 1 Your IP Server IP SYN
- 2 Server IP Your IP SYN, ACK
- 3 Your IP Server IP ACK

Click on each packet and expand:

- Transmission Control Protocol section



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY**(DTE CODE : 3470) (MSBTE Code : 1742)**Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

No.	Time	Source	Destination	Protocol	Length	Info
915	8.411937	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TCP	74	45231 → 443 [ACK] Seq=948 Ack=7136 Win=64256 Len=0
916	8.421405	2600:140f:c00::b854_	2409:40c2:2042:4122_	TLSv1.2	98	Application Data
917	8.422674	2600:140f:c00::b854_	2409:40c2:2042:4122_	TCP	74	443 → 44880 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
918	8.428090	10.97.187.222	4.240.189.64	TCP	66	45234 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
919	8.428894	64:ff9b::312c:cc23	2409:40c2:2042:4122_	TCP	86	443 → 45233 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
920	8.429136	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TCP	74	45233 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
921	8.433037	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TLSv1.2	291	Client Hello (SNI=kv601.prod.do.dsp.mp.microsoft.com)
922	8.434255	2409:40c2:2042:4122_	2600:140f:c00::b854_	TLSv1.3	154	Change Cipher Spec, Application Data
923	8.435451	2409:40c2:2042:4122_	2600:140f:c00::b854_	TLSv1.3	393	Application Data

0000 46 32 15 14 4e ee 40 f4 c9 c5 bb 61 08 00 45 00 F2-N@... a-E
0010 00 34 49 e1 40 00 80 06 28 73 0a 61 bb de 04 f0 4I@... (s a-
0020 bd 40 b8 b2 00 50 7a a9 ce 03 00 00 00 00 80 02 @... Pz-
0030 ff ff ec f0 00 00 02 04 05 b4 01 03 03 08 01 01 ..
0040 04 02

No.	Time	Source	Destination	Protocol	Length	Info
915	8.411937	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TCP	74	45231 → 443 [ACK] Seq=948 Ack=7136 Win=64256 Len=0
916	8.421405	2600:140f:c00::b854_	2409:40c2:2042:4122_	TLSv1.2	98	Application Data
917	8.422674	2600:140f:c00::b854_	2409:40c2:2042:4122_	TCP	74	443 → 44880 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
918	8.428090	10.97.187.222	4.240.189.64	TCP	66	45234 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
919	8.428894	64:ff9b::312c:cc23	2409:40c2:2042:4122_	TCP	86	443 → 45233 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
920	8.429136	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TCP	74	45233 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
921	8.433037	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TLSv1.2	291	Client Hello (SNI=kv601.prod.do.dsp.mp.microsoft.com)
922	8.434255	2409:40c2:2042:4122_	2600:140f:c00::b854_	TLSv1.3	154	Change Cipher Spec, Application Data
923	8.435451	2409:40c2:2042:4122_	2600:140f:c00::b854_	TLSv1.3	393	Application Data

0000 40 f4 c9 c5 bb 61 46 32 15 14 4e ee 86 dd 68 00 @... aF2-N-
0010 00 00 20 06 35 00 64 ff 9b 00 00 00 00 00 00 .. 5 d-
0020 00 00 31 2c cc 23 24 09 40 c2 20 42 41 22 c8 cb .., #\$_@ BA-
0030 54 a7 ee 87 f6 84 01 bb b0 b1 50 a3 67 fa 96 71 T-..-P g- q-
0040 13 b9 00 12 fa 99 7c 00 00 02 04 05 14 01 01 ..|
0050 04 02 01 03 03 07 ..

No.	Time	Source	Destination	Protocol	Length	Info
915	8.411937	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TCP	74	45231 → 443 [ACK] Seq=948 Ack=7136 Win=64256 Len=0
916	8.421405	2600:140f:c00::b854_	2409:40c2:2042:4122_	TLSv1.2	98	Application Data
917	8.422674	2600:140f:c00::b854_	2409:40c2:2042:4122_	TCP	74	443 → 44880 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
918	8.428090	10.97.187.222	4.240.189.64	TCP	66	45234 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
919	8.428894	64:ff9b::312c:cc23	2409:40c2:2042:4122_	TCP	86	443 → 45233 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
920	8.429136	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TCP	74	45233 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
921	8.433037	2409:40c2:2042:4122_	64:ff9b::312c:cc23	TLSv1.2	291	Client Hello (SNI=kv601.prod.do.dsp.mp.microsoft.com)
922	8.434255	2409:40c2:2042:4122_	2600:140f:c00::b854_	TLSv1.3	154	Change Cipher Spec, Application Data
923	8.435451	2409:40c2:2042:4122_	2600:140f:c00::b854_	TLSv1.3	393	Application Data

0000 46 32 15 14 4e ee 40 f4 c9 c5 bb 61 08 00 45 00 F2-N@... a-E
0010 c6 07 00 14 06 3f 24 09 40 c2 20 42 41 22 c8 cb .., ?\$@ BA-
0020 54 a7 ee 87 f6 84 00 64 ff 9b 00 00 00 00 00 .., #\$_@ P-
0030 00 00 31 2c cc 23 08 b1 01 bb 96 71 13 b9 50 a3 .., #\$_@ q- P-
0040 67 fb 50 10 00 ff d3 a0 00 00 .., g P- ..



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

☒ Objective

Understand how Application Layer protocols (DHCP, FTP, HTTP) behave using Wireshark, and how their headers and messages are structured within the TCP/IP stack.

☒ TCP/IP Layers (Recap)

TCP/IP Layer Example Protocols

Application HTTP, FTP, DHCP

Transport TCP, UDP

Network IP

Data Link Ethernet, Wi-Fi

We'll now focus on the Application Layer protocols.

❖ Step-by-Step Analysis in Wireshark

1. 🛡 DHCP (Dynamic Host Configuration Protocol)

⌚ Overview

- Used to automatically assign IP addresses to devices on a network.
- Operates over UDP ports 67 (server) and 68 (client).

⌚ How to Capture

1. Restart your computer's network connection (disable/enable Wi-Fi or Ethernet).
2. Start Wireshark before doing that.
3. Filter packets:
4. bootp

("bootp" is the filter for DHCP in Wireshark)

☒ What to Look For



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

You'll typically see:

- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP ACK

⌚ Header Format (in Wireshark)

Expand the packet sections:

- Bootstrap Protocol (BOOTP)
 - Message type (e.g., Boot Request/Reply)
 - Client IP, Your IP, Server IP
 - MAC address
- DHCP Options
 - Option 53: DHCP Message Type (Discover, Offer, etc.)
 - Option 1: Subnet Mask
 - Option 3: Router (Default Gateway)
 - Option 6: DNS Server



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

The screenshot shows a Wireshark capture window titled 'bootp'. The packet list pane displays several DHCP requests from a client (IP 10.0.0.0) to a broadcast address (255.255.255.255). The details pane shows the DHCP Request message structure, including fields like 'Message type: Boot Request (1)', 'Hardware type: Ethernet (0x01)', and 'Hardware address length: 6'. The bytes pane shows the raw hex and ASCII data of the captured packets. The status bar at the bottom indicates 'Packets: 4744 - Displayed: 3 (0.1%) - Dropped: 0 (0.0%)'.

2. FTP (File Transfer Protocol)

Overview

- Used to transfer files between client and server.
- Runs over TCP port 21 for commands, port 20 for data (active mode).

How to Capture

1. Start Wireshark.
2. Use an FTP client (like FileZilla) or command line:
3. `ftp ftp.dlptest.com`
4. Filter packets:
5. `ftp`

You'll see:

- FTP command/control packets (e.g., USER, PASS, LIST, RETR)
- FTP data transfer packets (on another TCP stream)

###



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

In the FTP section:

- Command: USER, PASS, LIST, etc.
- Response codes: 220, 331, 230, etc.

Expand the Transmission Control Protocol (TCP) section as well to see transport layer info.

3. HTTP (HyperText Transfer Protocol)

Overview

- Used for web communication.
- Uses TCP port 80 (HTTP) or 443 (HTTPS, not directly viewable unless decrypted).

How to Capture

1. Start Wireshark.
2. Open a browser and visit a non-HTTPS website like:
3. http://example.com
4. Filter packets:
5. http

What to Look For

You'll see:

- HTTP GET or POST requests
- HTTP 200 OK, 301 Redirect, 404 Not Found responses

HTTP Header Format (in Wireshark)

Expand the Hypertext Transfer Protocol section:

- HTTP Request:
- GET /index.html HTTP/1.1
- Host: example.com



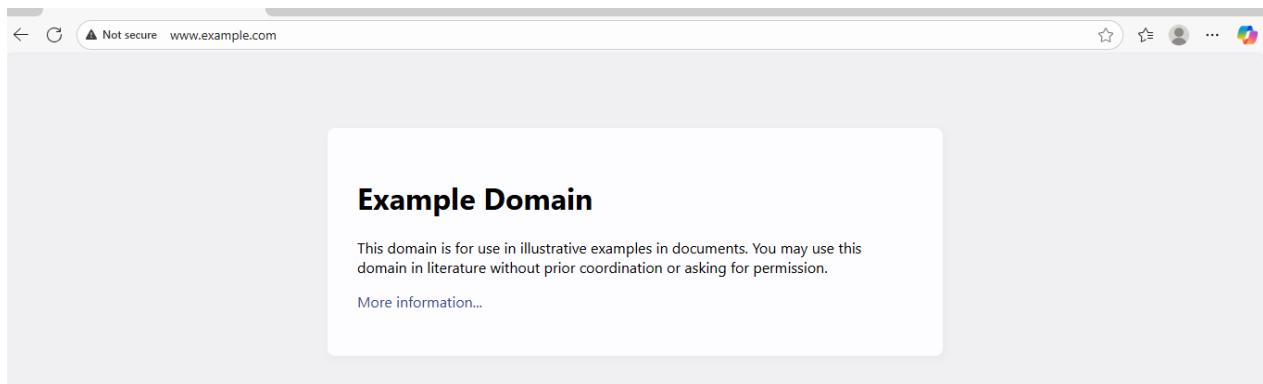
Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

- User-Agent: Mozilla/5.0
- Accept: text/html
- HTTP Response:
- HTTP/1.1 200 OK
- Content-Type: text/html
- Content-Length: 1256



```
http
No. Time Source Destination Protocol Length Info
1 478 11.436056 2409:40c2:2042:4122.. 2600:140f:c00::b854.. HTTP 530 GET / HTTP/1.1
2 667 15.884757 2600:140f:c00::b854.. 2409:40c2:2042:4122.. HTTP 1053 HTTP/1.1 200 OK (text/html)
3 689 15.355383 2409:40c2:2042:4122.. 2600:140f:c00::b854.. HTTP 474 GET /favicon.ico HTTP/1.1
4 724 16.354337 2600:140f:c00::b854.. 2409:40c2:2042:4122.. HTTP 422 HTTP/1.1 404 Not Found (text/html)

> Frame 478: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: FNLINKTECHNO_55:bb:61 (40:f4:c9:c5:bb:61), Dst: 46:32:15:14:4e:ee (46:32:15:14:4e:ee)
> Internet Protocol Version 6, Src: 2409:40c2:2042:4122:106e:ee76:2c6a:2bad, Dst: 2600:140f:c00::b854
> Transmission Control Protocol, Src Port: 45735, Dst Port: 80, Seq: 1, Ack: 1, Len: 456
< Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.example.com\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a...
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,en-IN;q=0.8\r\n
  \r\n
  [Response in frame: 667]
  [Full request URI: http://www.example.com/]

0000 46 32 15 14 4e ee 4f f4 c9 c5 bb 61 86 dd 60 0d F2::N@...:a`...
0010 20 07 01 dc 06 3f 24 09 4b c2 28 42 41 22 10 6e ...PS @:BA"-n
0020 ee 76 2c 6a 2b ad 26 00 14 0f 0c 00 00 00 00 00 -v,j+&.....
0030 00 00 b8 54 78 52 b2 a7 00 50 62 1d 8d 26 3d 16 -T-R- Pb-&-
0040 fe 49 50 18 00 ff 91 c6 00 00 47 45 54 28 2f 20 -IP.....GET /
0050 48 54 50 2f 31 2e 31 0d 08 48 6f 73 74 3a 20 HTTP/1.1 -Host:
0060 77 77 77 2e 65 61 6d 70 6c 65 29 63 6f 6d 0d www.example.com
0070 0d 43 6f 6c 66 65 73 64 69 6f 6e 3a 20 6b 65 65 -Connect ion: kee
0080 70 2d 61 6c 69 73 65 0d 0a 55 70 67 72 61 64 65 p-alive Upgrade
0090 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecu r-eReques
00a0 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65 6e ts: 1::User-Agent
00b0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 28 28 :Mozilla/5.0 (Windows NT 10.0;
00c0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 39 3b Win64; x64) App
00d0 20 57 69 36 34 3b 20 78 36 34 29 28 41 70 70 0de0 66 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 28 leWebKit/537.36
00f0 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec
0100 60 6f 29 20 43 68 72 67 6d 65 2f 31 34 30 2e 30 ko) Chrome/140.0
0110 2c 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e .0.0 SaFari/537.
0120 33 36 20 45 64 67 2f 31 34 30 2e 30 2e 30 2e 30 36 Edg/140.0.0.0
0130 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 -Accept: text/h
0140 74 6d 6c 62 61 70 76 6d 69 63 61 74 69 6f 6e 2f tml,application/
0150 78 68 74 6d 6c 2b 78 6d 6c 62 61 70 76 69 63 xhtml+xml, applic
0160 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 38 2e 39 2c ation/xm l;q=0.9,
0170 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 67 65 image/av if,image
0180 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 /webp,image/png
0190 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 6e 69 ,"/;q=0 .8,appli
01a0 63 61 74 69 6f 6a 73 6a 67 6a 2d 65 78 cation/c ioned-ev
```



Shri Yashwantrao Bhonsale Education Society's

YASHWANTRAO BHONSALE INSTITUTE OF TECHNOLOGY

(DTE CODE : 3470) (MSBTE Code : 1742)

Approved by AICTE, DTE & Affiliated to Mumbai University & MSBTE Mumbai
(NBA Accredited ME, CE, EE Diploma Programs)

Conclusion:

This practical exercise using Wireshark provided hands-on experience in analyzing the operation of the TCP/IP protocol suite across all layers. By capturing and inspecting network packets, the following key insights were gained:

- Ethernet Layer: Understanding of frame structures including source and destination MAC addresses and frame size, which forms the foundation for network communication at the data link level.
- Data Link Layer: Observation of MAC addresses and the ARP protocol demonstrated how devices map IP addresses to MAC addresses for local network communication.
- Network Layer: Detailed analysis of IP packet headers revealed how routing, fragmentation, and protocol identification occur. The ICMP protocol was explored through ping requests and replies, illustrating network diagnostics.
- Transport Layer: The TCP protocol's port numbers, flags, and the three-way handshake mechanism were studied, emphasizing how reliable connections are established and maintained.
- Application Layer: Protocols such as DHCP, FTP, and HTTP were analyzed, showing how IP configuration, file transfers, and web communications work at the application level, including their header formats.

Overall, Wireshark proved to be an essential tool for visualizing and understanding the complex processes of TCP/IP networking. This practical reinforced theoretical concepts by allowing real-time observation and analysis of network traffic, enhancing comprehension of how data flows through network layers in everyday internet communication.