| | |
|---|---|
| Batch: C2 | Roll No.:16010122323 |
| Experiment / assignment / tutorial No.10 | |
| Grade: AA / AB / BB / BC / CC / CD /DD | |
| **Signature of the Staff In-charge with date** | |

**Experiment No.:10**

# TITLE: Study of Packet Analyzer tool: Wireshark

**AIM:** To study and analyse various Protocols using Packet Analyzer tool: Wireshark

**Expected Outcome of Experiment:**
**CO:**

**Books/ Journals/ Websites referred:**

1. A. S. Tanenbaum, "Computer Networks", Pearson Education, Fourth Edition
2. B. A. Forouzan, "Data Communications and Networking", TMH, Fourth Edition

**Pre Lab/ Prior Concepts:**

IPv4 Addressing, Subnetting, Link State Protocol, Router configuration Commands

**New Concepts to be learned: Packet Analyzer tool: Wireshark.**

## THEORY:

### 1. Ethernet Frame

An Ethernet frame is a data packet that operates at the Data Link Layer (Layer 2) of the OSI model, used in wired LAN (Local Area Network) communication. It encapsulates data transmitted over Ethernet networks, providing reliable communication between devices on the same physical network.

**Ethernet Frame Structure:**

**Preamble (7 bytes): Synchronization pattern for frame alignment.**
**Start Frame Delimiter (SFD) (1 byte): Marks the start of the frame.**
**Destination MAC Address (6 bytes): The MAC address of the receiving device.**
**Source MAC Address (6 bytes): The MAC address of the sending device.**
**EtherType (2 bytes): Identifies the upper layer protocol (e.g., IPv4, IPv6, ARP).**
**Payload (46-1500 bytes): The actual data being transmitted, such as an IP packet.**
**Frame Check Sequence (FCS) (4 bytes): Used for error checking.**

**Types of Ethernet Frames:**

**Ethernet II Frame:** The most common Ethernet frame, identified by the EtherType field.
**IEEE 802.3 Frame:** Includes a length field rather than EtherType and is used in legacy networks.

**Advantages:**

Provides reliable LAN communication.

Efficient and standardized format for data transmission in wired networks.

**Disadvantages:**

Limited to local networks and cannot route across multiple networks like IP packets.

## 2. ICMP (Internet Control Message Protocol)

ICMP (Internet Control Message Protocol) is a network layer protocol used for error reporting and diagnostics in IP networks. ICMP is used by network devices to send control messages about network conditions, particularly during troubleshooting.

### Key Features:

**Error Reporting:** ICMP reports problems such as unreachable hosts, routers, or networks.
**Connectionless:** ICMP works independently of any connection state, making it a simple and lightweight protocol.
**Diagnostic Tool:** Commonly used in tools like ping and traceroute for connectivity checks and path tracing.

### Common ICMP Messages:

**Echo Request and Reply:** Used by ping to test network reachability.
Destination Unreachable: Reports when a packet cannot reach its destination.
Time Exceeded: Indicates that the packet's time-to-live (TTL) has expired**.**

### Advantages:

Helps diagnose network problems.
Simple and effective for error reporting.

### Disadvantages:

Can be exploited in DDoS (Distributed Denial of Service) attacks like ICMP floods.

### 3. ARP (Address Resolution Protocol)

ARP is a network layer protocol used to map an IP address to a MAC address in a local network. When a device needs to communicate with another device on the same network, it uses ARP to find the target device's MAC address if only the IP address is known.

**ARP Process:**

**ARP Request**: A broadcast message is sent to all devices on the network, asking which device has a specific IP address.

**ARP Reply:** The device with the matching IP address responds with its MAC address.

**Types of ARP:**

**Gratuitous ARP:** A device announces its own IP-MAC mapping to update other devices.

**Proxy ARP:** A router replies to ARP requests on behalf of devices on another network.

**Advantages:**

Allows dynamic mapping between IP and MAC addresses.
Essential for communication within a local network.

**Disadvantages:**

Vulnerable to ARP spoofing attacks, where attackers send fake ARP replies.

### 3. IP Header (Internet Protocol Header)

The IP header is a part of the IP packet, which operates at the network layer (Layer 3). It contains metadata about the packet, including addressing

and control information, enabling packet delivery from source to destination.

**Structure of IPv4 Header:**

Version (4 bits): Specifies the IP version (IPv4 or IPv6).
Header Length (4 bits): Indicates the size of the header.
Type of Service (TOS) (8 bits): Specifies packet priority.
Total Length (16 bits): The total length of the IP packet.
Identification (16 bits): A unique identifier for fragmented packets.
Flags (3 bits): Control fragmentation.
Fragment Offset (13 bits): Indicates the fragment's position.
Time to Live (TTL) (8 bits): Limits the packet's lifetime.
Protocol (8 bits): Specifies the transport layer protocol (TCP, UDP).
Header Checksum (16 bits): Error-checking for the header.
Source IP Address (32 bits): The IP address of the sender.
Destination IP Address (32 bits): The IP address of the receiver.

**Advantages:**

Enables routing of packets across different networks.
Facilitates fragmentation and reassembly of large packets.

**Disadvantages:**

Overhead due to the inclusion of control information.
Vulnerable to attacks like IP spoofing.

**5. TCP (Transmission Control Protocol)**

TCP is a transport layer protocol that provides reliable, connection-oriented communication between devices. It ensures that data is delivered accurately and in the correct order.

**Key Features:**

**Connection-Oriented:** TCP establishes a connection before data transfer (via a three-way handshake).

**Reliability:** Guarantees data delivery without errors, duplication, or loss.
**Flow Control:** Adjusts the data transmission rate based on the receiver's capacity.
**Error Detection and Recovery:** TCP detects errors using checksums and resends lost or damaged segments.

**TCP Handshake Process:**

SYN: The client sends a SYN packet to initiate a connection.
SYN-ACK: The server responds with a SYN-ACK packet.
ACK: The client acknowledges the server's response, and the connection is established.

**Advantages:**

Reliable and ensures accurate data transmission.
Provides flow and congestion control mechanisms.

**Disadvantages:**

High overhead due to error correction and connection management, making it slower than UDP.

**6. UDP (User Datagram Protocol)**

UDP is a transport layer protocol that provides connectionless and unreliable communication. It is faster and simpler than TCP but does not guarantee the delivery or correct ordering of data.

**Key Features:**

**Connectionless:** UDP does not establish a connection before sending data.
**Unreliable**: Data delivery is not guaranteed, and packets may be lost or arrive out of order.

**Low Overhead:** UDP is faster because it lacks error correction and flow control mechanisms.

**UDP Packet Structure:**
Source Port: Identifies the sending port.
Destination Port: Identifies the receiving port.
Length: Specifies the length of the UDP header and data.
Checksum: Used for error-checking.

Common Uses:

Real-time applications like video streaming, VoIP, and online gaming.
DNS queries where speed is more critical than reliability.

**Advantages:**

Low overhead and faster transmission.

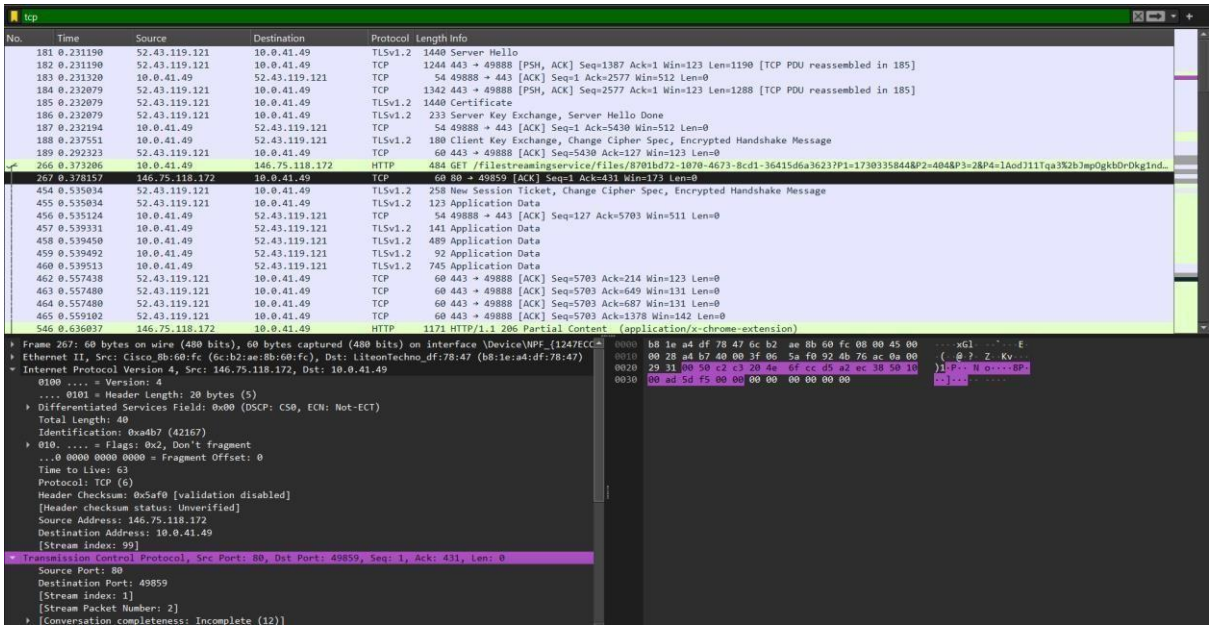
Suitable for real-time, loss-tolerant applications.

**Disadvantages:**

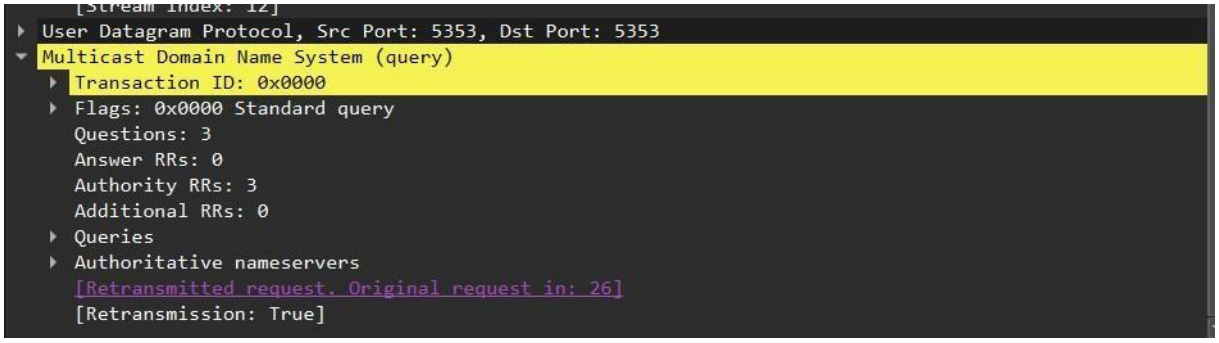
No guarantee of data delivery, order, or error recovery.

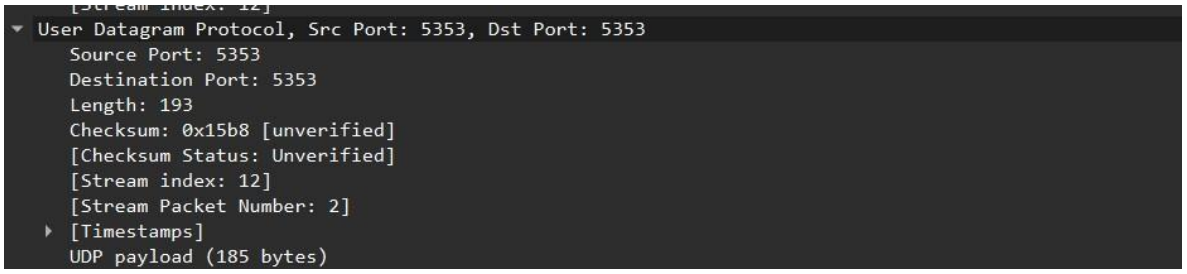
**IMPLEMENTATION:**

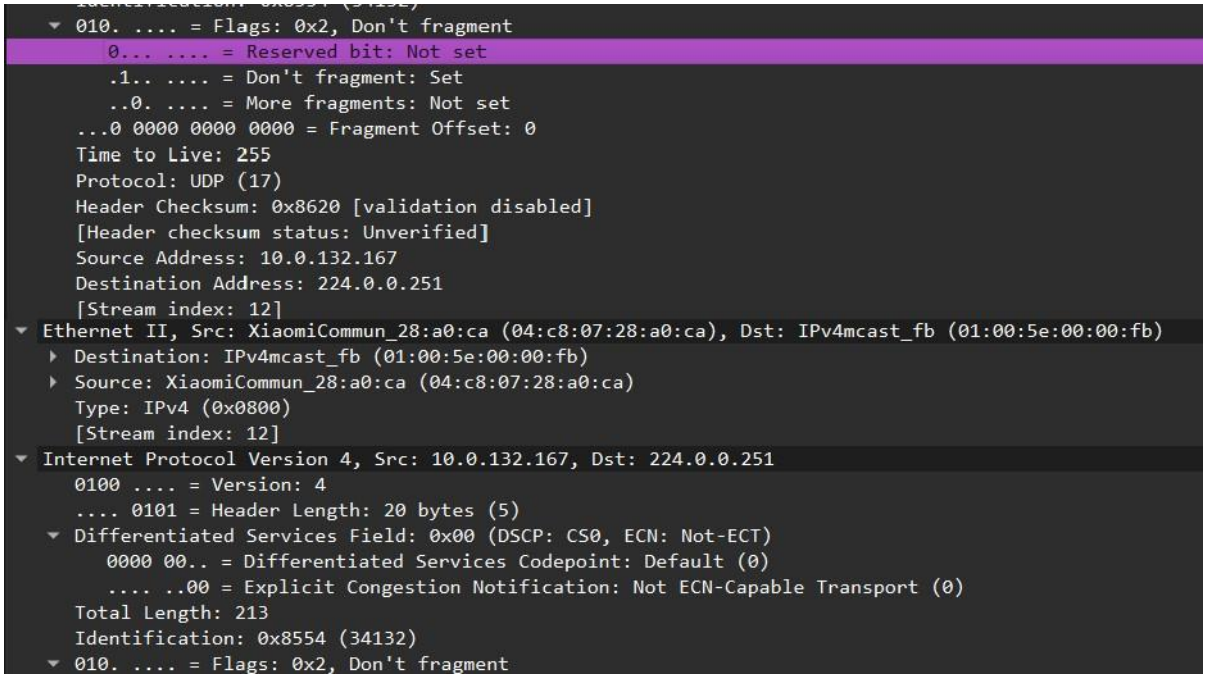
**TCP**


tcp
No. Time Source Destination Protocol Length Info
181 0.231190 52.43.119.121 10.0.41.49 TLSv1.2 1440 Server Hello
182 0.231190 52.43.119.121 10.0.41.49 TCP 1244 443 → 49888 [PSH, ACK] Seq=1387 Ack=1 Win=123 Len=1190 [TCP PDU reassembled in 185]
183 0.231320 10.0.41.49 52.43.119.121 TCP 54 49888 → 443 [ACK] Seq=1 Ack=2577 Win=512 Len=0
184 0.232079 52.43.119.121 10.0.41.49 TCP 1342 443 → 49888 [PSH, ACK] Seq=2577 Ack=1 Win=123 Len=1288 [TCP PDU reassembled in 185]
185 0.232079 52.43.119.121 10.0.41.49 TLSv1.2 1440 Certificate
186 0.232079 52.43.119.121 10.0.41.49 TLSv1.2 233 Server Key Exchange, Server Hello Done
187 0.232194 10.0.41.49 52.43.119.121 TCP 54 49888 → 443 [ACK] Seq=1 Ack=5430 Win=512 Len=0
188 0.237551 10.0.41.49 52.43.119.121 TLSv1.2 180 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
189 0.292323 52.43.119.121 10.0.41.49 TCP 60 443 → 49888 [ACK] Seq=5430 Ack=127 Win=123 Len=0
266 0.373206 10.0.41.49 146.75.118.172 HTTP 484 GET /filestreamingservice/files/8701bd72-1070-4673-8cd1-36415d6a3623?P1=1730335844&P2=404&P3=2&P4=1AodJ11Tqa3%2bJmpOgkbOrDkg1nd…
267 0.378157 146.75.118.172 10.0.41.49 TCP 60 80 → 49859 [ACK] Seq=1 Ack=431 Win=173 Len=0
454 0.535034 52.43.119.121 10.0.41.49 TLSv1.2 258 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
455 0.535034 52.43.119.121 10.0.41.49 TLSv1.2 123 Application Data
456 0.535124 10.0.41.49 52.43.119.121 TCP 54 49888 → 443 [ACK] Seq=127 Ack=5703 Win=511 Len=0
457 0.539331 10.0.41.49 52.43.119.121 TLSv1.2 141 Application Data
458 0.539450 10.0.41.49 52.43.119.121 TLSv1.2 489 Application Data
459 0.539492 10.0.41.49 52.43.119.121 TLSv1.2 92 Application Data
460 0.539513 10.0.41.49 52.43.119.121 TLSv1.2 745 Application Data
462 0.557438 52.43.119.121 10.0.41.49 TCP 60 443 → 49888 [ACK] Seq=5703 Ack=214 Win=123 Len=0
463 0.557480 52.43.119.121 10.0.41.49 TCP 60 443 → 49888 [ACK] Seq=5703 Ack=649 Win=131 Len=0
464 0.557480 52.43.119.121 10.0.41.49 TCP 60 443 → 49888 [ACK] Seq=5703 Ack=687 Win=131 Len=0
465 0.559102 52.43.119.121 10.0.41.49 TCP 60 443 → 49888 [ACK] Seq=5703 Ack=1378 Win=142 Len=0
546 0.636037 146.75.118.172 10.0.41.49 HTTP 1171 HTTP/1.1 206 Partial Content (application/x-chrome-extension)
Frame 267: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{1247ECC
Ethernet II, Src: Cisco_8b:60:fc (6c:b2:ae:8b:60:fc), Dst: LiteonTechno_df:78:47 (b8:1e:a4:df:78:47)
Internet Protocol Version 4, Src: 146.75.118.172, Dst: 10.0.41.49
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0xa4b7 (42167)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: TCP (6)
Header Checksum: 0x5af0 [validation disabled]
[Header checksum status: Unverified]
Source Address: 146.75.118.172
Destination Address: 10.0.41.49
[Stream index: 99]
Transmission Control Protocol, Src Port: 80, Dst Port: 49859, Seq: 1, Ack: 431, Len: 0
Source Port: 80
Destination Port: 49859
[Stream index: 1]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (12)]
0000 b8 1e a4 df 78 47 6c b2 ae 8b 60 fc 08 00 45 00 ····xGl· ··`···E·
0010 00 28 a4 b7 40 00 3f 06 5a f0 92 4b 76 ac 0a 00 ·(··@·?· Z··Kv···
0020 29 31 00 50 c2 c3 20 4e 6f cc d5 a2 ec 38 50 10 )1·P·· N o····8P·
0030 00 ad 5d f5 00 00 00 00 00 00 00 00 ··]·····

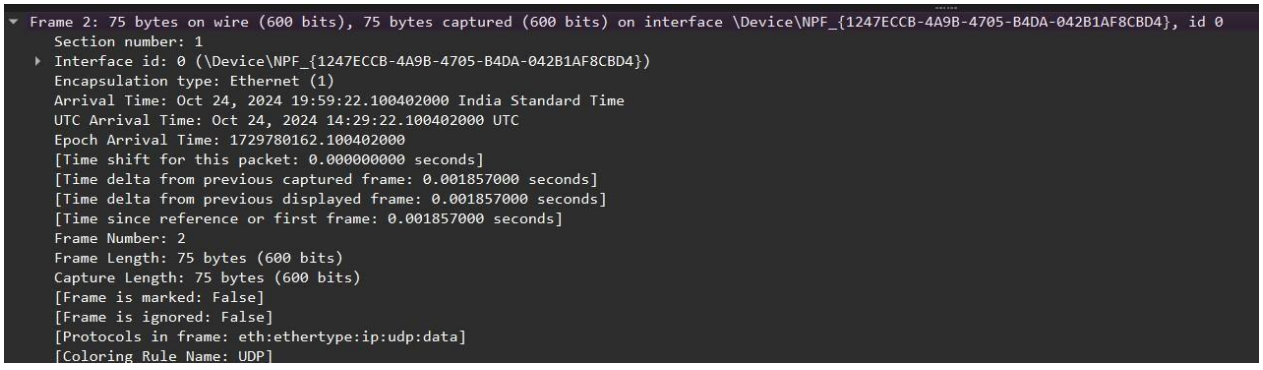

Source Port: 80
Destination Port: 49859
[Stream index: 1]
[Stream Packet Number: 2]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 542011340
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 431 (relative ack number)
Acknowledgment number (raw): 3584224312
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 173
[Calculated window size: 173]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x5df5 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 266]
[The RTT to ACK the segment was: 0.004951000 seconds]
0000 b8 1e a4 df 78 47 6c b2 ae 8b 60 fc 08 00 45 00 ····xGl· ··`···E·
0010 00 28 a4 b7 40 00 3f 06 5a f0 92 4b 76 ac 0a 00 ·(··@·?· Z··Kv···
0020 29 31 00 50 c2 c3 20 4e 6f cc d5 a2 ec 38 50 10 )1·P·· N o····8P·
0030 00 ad 5d f5 00 00 00 00 00 00 00 00 ··]·····

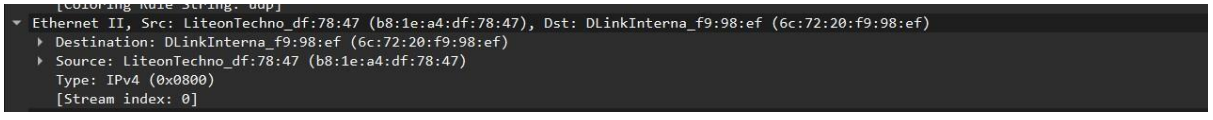

[Stream index: 12]
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
Transaction ID: 0x0000
Flags: 0x0000 Standard query
Questions: 3
Answer RRs: 0
Authority RRs: 3
Additional RRs: 0
Queries
Authoritative nameservers
[Retransmitted request. Original request in: 26]
[Retransmission: True]


[Stream index: 12]
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Source Port: 5353
Destination Port: 5353
Length: 193
Checksum: 0x15b8 [unverified]
[Checksum Status: Unverified]
[Stream index: 12]
[Stream Packet Number: 2]
[Timestamps]
UDP payload (185 bytes)


010. .... = Flags: 0x2, Don't fragment
0... .... = Reserved bit: Not set
.1.. .... = Don't fragment: Set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: UDP (17)
Header Checksum: 0x8620 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.132.167
Destination Address: 224.0.0.251
[Stream index: 12]
Ethernet II, Src: XiaomiCommun_28:a0:ca (04:c8:07:28:a0:ca), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Destination: IPv4mcast_fb (01:00:5e:00:00:fb)
Source: XiaomiCommun_28:a0:ca (04:c8:07:28:a0:ca)
Type: IPv4 (0x0800)
[Stream index: 12]
Internet Protocol Version 4, Src: 10.0.132.167, Dst: 224.0.0.251
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 213
Identification: 0x8554 (34132)
010. .... = Flags: 0x2, Don't fragment

## UDP


Frame 2: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{1247ECCB-4A9B-4705-B4DA-042B1AF8CBD4}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{1247ECCB-4A9B-4705-B4DA-042B1AF8CBD4})
Encapsulation type: Ethernet (1)
Arrival Time: Oct 24, 2024 19:59:22.100402000 India Standard Time
UTC Arrival Time: Oct 24, 2024 14:29:22.100402000 UTC
Epoch Arrival Time: 1729780162.100402000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.001857000 seconds]
[Time delta from previous displayed frame: 0.001857000 seconds]
[Time since reference or first frame: 0.001857000 seconds]
Frame Number: 2
Frame Length: 75 bytes (600 bits)
Capture Length: 75 bytes (600 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:data]
[Coloring Rule Name: UDP]

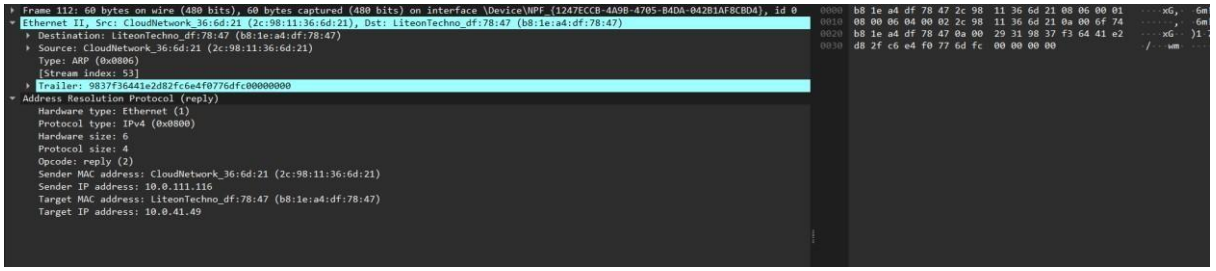

Ethernet II, Src: LiteonTechno_df:78:47 (b8:1e:a4:df:78:47), Dst: DLinkInterna_f9:98:ef (6c:72:20:f9:98:ef)
Destination: DLinkInterna_f9:98:ef (6c:72:20:f9:98:ef)
Source: LiteonTechno_df:78:47 (b8:1e:a4:df:78:47)
Type: IPv4 (0x0800)
[Stream index: 0]

```
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 142.250.66.14
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 61
    Identification: 0xbd85 (48517)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xab75 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.4
    Destination Address: 142.250.66.14
    [Stream index: 0]
```

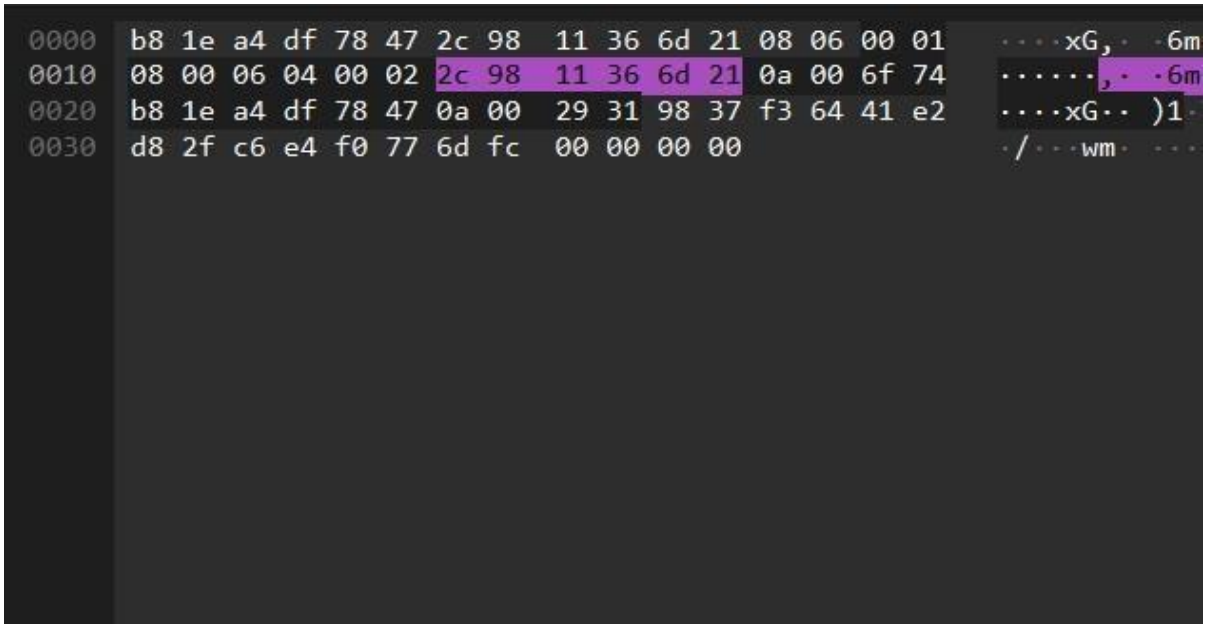
```
User Datagram Protocol, Src Port: 52440, Dst Port: 443
    Source Port: 52440
    Destination Port: 443
    Length: 41
    Checksum: 0x4111 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 2]
  ▸ [Timestamps]
    UDP payload (33 bytes)
```

```
Data (33 bytes)
    Data: 4ae0323ffbff406c175f9cfda32bcd14cdea9b21c566bed4c3c8da231cf9afeb28
    [Length: 33]
```

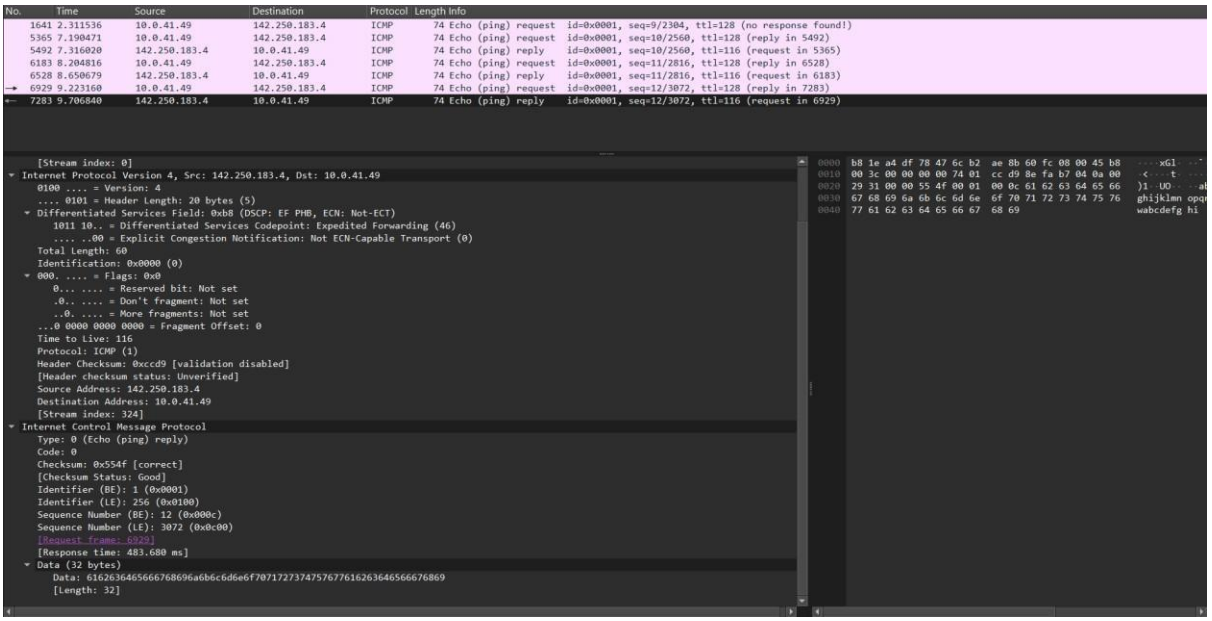
## ARP




```
Frame 112: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{1247ECCB-4A9B-4705-B4DA-042B1AF8CBD4}, id 0
Ethernet II, Src: CloudNetwork_36:6d:21 (2c:98:11:36:6d:21), Dst: LiteonTechno_df:78:47 (b8:1e:a4:df:78:47)
  ▸ Destination: LiteonTechno_df:78:47 (b8:1e:a4:df:78:47)
  ▸ Source: CloudNetwork_36:6d:21 (2c:98:11:36:6d:21)
    Type: ARP (0x0806)
    [Stream index: 53]
  ▸ Trailer: 9837f36441e2d82fc6e4f0776dfc00000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: CloudNetwork_36:6d:21 (2c:98:11:36:6d:21)
    Sender IP address: 10.0.111.116
    Target MAC address: LiteonTechno_df:78:47 (b8:1e:a4:df:78:47)
    Target IP address: 10.0.41.49
```




## ICMP:




**Date:** **Signature of faculty in-charge**