

# Wireshark Lab 2: HTTP – Part 1: Basic IPv4

**Name:** Muhammad Shoaib Ahmad

**Course:** Computer Networking

**Lab Title:** Wireshark Lab 2 – IP (Part 1: IPv4)

---

## Instructions:

- Answers are provided based on the reference file ip-wireshark-trace1-1.pcapng.
- 



### Question 1:

**What is the IP address of your computer?**



#### Answer:

192.168.86.61

---



### Question 2:

**What is the value in the Time-To-Live (TTL) field in this IPv4 datagram's header?**



#### Answer:

1

Same as Q1 or crop TTL part. Highlight **TTL: 1**.

---



### Question 3:

**What is the value in the upper-layer protocol field in this IPv4 datagram's header?**



#### Answer:

17 (UDP)

```

Wireshark - Packet 6 - ip-wireshark-trace1.pcapng

Frame 6: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF_{993B6949-3DEB-40E5-BEA3-FB993A5D7C3E}, id 0
Ethernet II, Src: InfinityWire_63:e0:f8 (3c:46:17:63:e0:f8), Dst: Intel_06:a7:39 (7d:48:3e:06:a7:39)
Internet Protocol Version 4, Src: 172.217.17.74, Dst: 192.168.10.9
User Datagram Protocol, Src Port: 443, Dst Port: 5236
  QUIC IETF
    QUIC Connection information
      [Packet Length: 1250]
        .1.... = Header Form: Long Header (1)
        .1.... = Fixed Bit: True
        .00.... = Packet Type: Initial (0)
        [...] 00... = Reserved: 0
      ...
0x0030 08 fd 73 e9 9d 1d f0 97 0f 00 44 d8 3d 41 44 4e  s..... D=ADN
0x0040 ab 16 e2 a9 f0 db 14 26 3e 2b b0 f0 19 c9 10 b5 .....<8>+.....
0x0050 9a 4a 1c 66 16 67 a6 a6 49 39 73 1e 0a 24 99 J-f,g] I95-$
0x0060 58 87 50 9f 1a 16 c2 a5 c7 b4 07 3a 45 18 a8 d0 X-P..... .1.....
0x0070 ea b0 a9 eb ff 39 fc 6a 3f 72 7a 00 42 9d a2 .....9 j;r,z-B-
0x0080 cc f8 80 7e f5 28 81 32 ce fb 9c 11 ed c1 b2 a2 ..L->x-2 .....
0x0090 c1 d1 57 90 9f 9f bf 9c 20 35 05 7d 05 d9 25 ..W-.-. 5-z-%
0x00a0 ad 90 90 48 3d et et fa 3d 04 d6 26 8a ..H2 <-8+R+
0x00b0 1c ee 84 88 4a 13 14 8b c1 0b 0b 0b 0b 0b 0b 0b ..J.....
0x00c0 08 77 84 7b 9a 04 e9 58 ..c2 28 7c 3d 7d 96 ..{..-X ..|=-.
0x00d0 b5 14 6d be d0 99 4b 12 ba 2c b6 ad e9 98 15 ..m...-D ..|=-.
0x00e0 1e fd 82 03 0d 33 df 70 88 bf 7e 1c 2b 28 ce 70 ..3-p ..++ .p
0x00f0 23 0e 9e d3 c7 5e da 96 bb 6f b4 3e 11 ff 9f 8d #....^.. o->...
0x0100 83 ed 94 bf 74 eb 13 14 2b a5 57 ae 89 8b cc 0c ..t.... +W....
0x0110 00 66 71 b2 29 ff bb 0f ca 12 22 8c 61 26 e7 1c ..(fq)... .."-ak&-
0x0120 81 dd bc 6c 62 8f bf 04 a3 e4 57 37 5e e6 3e 38 ..lb... T-7->8
0x0130 fb ef 56 6f 28 40 8b 9c a5 a1 24 bd 04 62 51 9e ..\o@... ..bQ-
0x0140 bd 4c ed b1 02 4b 85 95 na 04 e8 5c b7 20 b9 6f ..L...K- Z..`..o
0x0150 89 72 87 ee 44 8a 14 2b 23 b7 b4 94 16 ca 63 62 ..r...-D... #...-cb
0x0160 57 23 89 c4 6d 29 85 16 d9 8a fa 8b 53 3d 32 88 W#..-m)... ..S-2.
0x0170 c4 38 f8 08 d2 76 82 af 60 98 1e 72 fd 34 01 4e ..0...v... ..r...-4-N
0x0180 61 9b 5e 33 c7 a5 5d c9 5d 2f 32 ad 1a 13 a.^3-.. ]}2/...
0x0190 48 3d c9 7f ff b4 03 d6 61 39 fb 02 d5 01 26 c2 d2 H=-.a 9...&-
0x01a0 ee be 56 d8 17 91 25 2f 78 9d 65 ac 67 81 14 ..V...% /x-e.g-
0x01b0 f3 95 4a 04 07 95 9c 71 4b 49 4c ff d3 96 bd 92 ..J...-q KIL...
0x01c0 4a e2 98 39 a9 79 4f 16 52 e8 ea 45 d8 e0 61 J...-9.y0 R...-E..-a
0x01d0 ee b3 82 f4 f2 20 27 29 88 1c 48 c1 44 80 88 7d ..(..... ) ..-H.M-..}
0x01e0 6a b2 f5 a6 3b d5 8b cf ab d5 ce 01 16 1f cc j...;.. ..-.
0x01f0 90 62 77 72 73 72 72 72 72 72 72 72 72 72 72 72 ..0...-r... ..-gu-$
0x0200 02 62 77 72 73 72 72 72 72 72 72 72 72 72 72 72 ..b...-r... ..-S-.
0x0210 28 28 28 28 77 62 c7 b6 ..c0 f4 a0 00 00 17 21 b8 @(-.wb... ..I-..-.
0x0220 6a 09 65 6e 88 ff 7f 17 ec 49 lf ff 78 72 cc 59 j-en... ..I-xr-P
0x0230 0b ce a3 8f 72 d6 52 9e 53 96 cd 5f 9e 5e 59 3f ..r-R.. S...-Y?
0x0240 dc a7 5c d1 29 81 c3 3b cd 6d ab ea e1 5f 3c 37 ..`..;.. m...<7
```

 **Question 4:**

**How many bytes are in the IP header?**

 **Answer:**

20 bytes

## Explanation:

This is the standard size of an IP header without any options. Wireshark shows Header Length: 20 bytes

```
[Packet Length: 1250]
1.... .... = Header Form: Long Header (1)
.1... .... = Fixed Bit: True
..00 .... = Packet Type: Initial (0)
[.... 00.. = Reserved: 0]
[.... ..00 = Packet Number Length: 1 bytes (0)]
Version: 1 (0x00000001)
Destination Connection ID Length: 0
Source Connection ID Length: 8
Source Connection ID: fd73e99d1df0970f
Token Length: 0
Length: 1250
```

---

## Question 5:

How many bytes are in the payload of the IP datagram?

### Answer:

28 bytes

### Explanation:

The **Total Length** of the IP datagram is **48 bytes**. Subtracting the **20-byte header**, we get **28 bytes payload**.

---

## Question 6:

Has this IP datagram been fragmented? Explain.

### Answer:

No, the "More Fragments" flag is set to **0** and the **Fragment Offset** is also **0**.

```
► Ethernet II, Src: InfinityWire_63:e0:f8 (3c:46:45:63:e0:f8), Dst: Intel_06:a7:39 (74:d8)
▼ Internet Protocol Version 4, Src: 172.217.17.74, Dst: 192.168.10.9
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  ▶ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 61
    Protocol: UDP (17)
    Header Checksum: 0xb4e4 [validation disabled]
      [Header checksum status: Unverified]
    Source Address: 172.217.17.74
    Destination Address: 192.168.10.9
      [Stream index: 0]
▼ User Datagram Protocol, Src Port: 443, Dst Port: 52336
  Source Port: 443
  Destination Port: 52336
  Length: 32
  Checksum: 0xe89e [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 11]
  ▶ [Timestamps]
  UDP payload (24 bytes)
▼ QUIC IETF
  QUIC Connection Information
```

---

## Question 7:

Which fields in the IP datagram change from one datagram to the next in the UDP sequence? Why?

### Answer:

- **Identification** field
- **TTL**
- **Header checksum**

### Explanation:

Each datagram is a new packet, hence Identification and Checksum are unique. TTL increases because each traceroute hop sends a new packet with a higher TTL.

---

## Question 8:

Which fields stay constant in the UDP datagram sequence? Why?

### Answer:

- **Source IP:** 192.168.86.61
- **Destination IP:** 128.119.245.12
- **Protocol:** UDP (17)

```
▼ User Datagram Protocol, Src Port: 443, Dst Port: 52336
  Source Port: 443
  Destination Port: 52336
  Length: 1258
  Checksum: 0x838a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Stream Packet Number: 6]
  ▶ [Timestamps]
  UDP payload (1250 bytes)
▼ QUIC IETF
```

### Explanation:

Because the packets are being sent from the same source to the same destination using the same transport layer protocol.

---

 **Question 9:**

**Describe the pattern in the values in the Identification field of the IP datagrams.**

 **Answer:**

The **Identification field increases sequentially** by 1 with each new datagram (e.g., 0x2c26, 0x2c27, 0x2c28, ...).

 **Explanation:**

This is standard behavior as each packet is uniquely identified for potential fragmentation reassembly.

---

 **Question 10:**

**What is the upper layer protocol in the IP datagrams returned from routers (ICMP replies)?**

 **Answer:**

**1 (ICMP)**

---

 **Question 11:**

**Are the Identification values in ICMP packets similar in behavior to Q9?**

 **Answer:**

No. The **Identification field varies** non-sequentially in ICMP responses because each router independently generates its own IP datagrams.

---

 **Question 12:**

**Are TTL values similar across all ICMP packets from routers?**

 **Answer:**

**No.** The TTL values are generally **high (often 64 or 128)** depending on the router OS, and not sequential or incrementing like outgoing packets.

## **Explanation:**

Routers reply with TTLs from their own OS default, unrelated to the original TTL values used in traceroute.

```
Arrival Time: May 10, 2025 22:09:50.416317000 Pakistan Standard Time
UTC Arrival Time: May 10, 2025 17:09:50.416317000 UTC
Epoch Arrival Time: 1746896990.416317000
[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: 0.212507000 seconds]
Frame Number: 14
Frame Length: 66 bytes (528 bits)
Capture Length: 66 bytes (528 bits)
[Frame is marked: False]
[Frame is ignored: False]
```

---

## Fragmentation

---

### **Q13. Has that segment been fragmented across more than one IP datagram?**

#### **Answer:**

Yes, the 3000-byte UDP segment has been fragmented into three IP datagrams (packet numbers 179, 180, and 181 in the trace file).

178 12.457300 192.168.10.9	142.250.181.46	QUIC	1292 Initial, DCID=eb102d107003a6cf, PKN: 6, PADDING, PI
179 12.475309 142.250.181.46	192.168.10.9	QUIC	1292 Initial, SCID=eb102d107003a6cf, PKN: 5, CRYPTO, PAD
180 12.478145 142.250.181.46	192.168.10.9	QUIC	341 Protected Payload (KP0)
181 12.478664 142.250.181.46	192.168.10.9	QUIC	993 Protected Payload (KP0)
182 12.479198 142.250.181.46	192.168.10.9	QUIC	80 Protected Payload (KP0)
183 12.479378 192.168.10.9	142.250.181.46	QUIC	1292 Handshake, DCID=eb102d107003a6cf
184 12.479706 192.168.10.9	142.250.181.46	QUIC	73 Protected Payload (KP0), DCID=eb102d107003a6cf
185 12.480368 192.168.10.9	142.250.181.46	QUIC	456 Protected Payload (KP0), DCID=eb102d107003a6cf

---

### **Q14. What information in the IP header indicates that this datagram has been fragmented?**

#### **Answer:**

The "More Fragments" flag is set to 1, and the Fragment Offset field is greater than 0 for the second and third packets. These indicate that fragmentation has occurred.

```
▼ Internet Protocol Version 4, Src: 142.250.181.46, Dst: 192.168.10.9
  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: 1278
  Identification: 0x0000 (0)
▼ 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: 60
  Protocol: UDP (17)
  Header Checksum: 0x2b15 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 142.250.181.46
  Destination Address: 192.168.10.9
  [Stream index: 12]
▼ User Datagram Protocol, Src Port: 443, Dst Port: 51411
```

---

### Q15. What indicates whether this is the first fragment versus a latter fragment?

#### Answer:

The first fragment has **Fragment Offset = 0**. Later fragments have a **non-zero Fragment Offset**, and only the first fragment contains the **UDP header**.

---

### Q16. How many bytes are in this IP datagram (header + payload)?

#### Answer:

The first fragment (packet 179) has a **Total Length** of **1500 bytes**, which includes 20-byte IP header and 1480 bytes of data.

---

### Q17. What indicates that this is not the first datagram fragment?

#### Answer:

The second fragment (packet 180) has a **non-zero Fragment Offset** and **does not contain a UDP header**.

---

### Q18. What fields change in the IP header between the first and second fragments?

### Answer:

The fields that change:

- **Total Length**
- **Fragment Offset**
- **More Fragments flag**
- **Header Checksum**

The **Identification field remains the same** (because all fragments belong to the same original datagram).

---

### Q19. What indicates that this is the last fragment of the segment?

#### Answer:

In the last fragment (packet 181), the **More Fragments flag = 0**. This means it is the final part of the original datagram.

The screenshot shows the Wireshark interface with the following details for Frame 181:

- Frame number:** 181
- Length:** 993 bytes on wire (7944 bits), 993 bytes captured (7944 bits) on interface \Device\NPF\_{993B6949-3DEB-40E5-BEA3-FB993A5D7C3E}
- Section number:** 1
- Interface id:** 0 (\Device\NPF\_{993B6949-3DEB-40E5-BEA3-FB993A5D7C3E})
  - Interface name:** \Device\NPF\_{993B6949-3DEB-40E5-BEA3-FB993A5D7C3E}
  - Interface description:** Wi-Fi
  - Encapsulation type:** Ethernet (1)
  - Arrival Time:** May 10, 2025 22:10:02.682474000 Pakistan Standard Time
  - UTC Arrival Time:** May 10, 2025 17:10:02.682474000 UTC
  - Epoch Arrival Time:** 1746897002.682474000
  - [Time shift for this packet: 0.000000000 seconds]
  - [Time delta from previous captured frame: 0.000519000 seconds]
  - [Time delta from previous displayed frame: 0.000519000 seconds]
  - [Time since reference or first frame: 12.478664000 seconds]
- Frame Number:** 181
- Frame Length:** 993 bytes (7944 bits)
- Capture Length:** 993 bytes (7944 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:ip:udp:quic]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]
- Ethernet II:** Src: InfinityWire\_63:e0:f8 (3c:46:45:63:e0:f8), Dst: Intel\_06:a7:39 (74:d8:3e:06:a7:39)
  - Destination:** Intel\_06:a7:39 (74:d8:3e:06:a7:39)
    - .... 0. .... .... .... = LG bit: Globally unique address (factory default)
    - .... 0. .... .... .... = IG bit: Individual address (unicast)
  - Source:** InfinityWire\_63:e0:f8 (3c:46:45:63:e0:f8)
    - .... 0. .... .... .... = LG bit: Globally unique address (factory default)
    - .... 0. .... .... .... = IG bit: Individual address (unicast)
- Hex View:** Shows the raw byte sequence of the packet.
- Text View:** Shows the ASCII representation of the packet.
- Details View:** Shows detailed information for each field in the packet.
- Summary View:** Shows a summary of the packet's contents.
- File View:** Shows options for saving the packet.
- Help View:** Shows help and documentation options.

## Question 20:

What is the IPv6 address of the computer making the DNS AAAA request?

### Answer:

2001:558:6006:5f:69c6:6994:7a02:db6c

 *Explanation:* This is the source address of packet #20 in the trace.

```
▶ Frame 95: 102 bytes on wire (816 bits), 102 bytes captured (81
▶ Ethernet II, Src: GuangzhouShi_93:ab:69 (58:41:46:93:ab:69), D
▶ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 224.0.0.2
▶ User Datagram Protocol, Src Port: 5353, Dst Port: 5353
▶ Multicast Domain Name System (query)
```

---

## Question 21:

What is the IPv6 destination address for this datagram?

### Answer:

2001:558:feed::1

 *Explanation:* This is the IPv6 address of the DNS server queried.

```
Wireshark - Packet 55 - WiFi  
  
Total Length: 88  
Identification: 0x6fad (28589)  
► 010. .... = Flags: 0x2, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 255  
Protocol: UDP (17)  
Header Checksum: 0x6041 [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 192.168.10.2  
Destination Address: 224.0.0.251  
[Stream index: 8]  
► User Datagram Protocol, Src Port: 5353, Dst Port: 5353
```

---

### 💡 Question 22:

**What is the value of the flow label for this datagram?**

📝 **Answer:**

0x63d51

📘 *Explanation:* Found under the IPv6 header → Flow Label field in Wireshark.

---

### 💡 Question 23:

**How much payload data is carried in this datagram?**

📝 **Answer:**

73 bytes

📘 *Explanation:* The Payload Length field of the IPv6 header is 73.

Wireshark - Packet 95 · WI-FI

Frame 95: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface  
Section number: 1

Interface id: 0 (\Device\NPF\_{993B6949-3DEB-40E5-BEA3-FB993A5D7C3E})  
Encapsulation type: Ethernet (1)  
Arrival Time: May 10, 2025 22:50:26.419192000 Pakistan Standard Time  
UTC Arrival Time: May 10, 2025 17:50:26.419192000 UTC  
Epoch Arrival Time: 1746899426.419192000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 0.128792000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 19.980787000 seconds]  
Frame Number: 95  
Frame Length: 102 bytes (816 bits)  
Capture Length: 102 bytes (816 bits)

0000 01 00 5e 00 00 fb 58 41 46 93 ab 69 08 00 45 00 . . . X A F . i . E .  
0010 00 58 6f ad 40 00 ff 11 60 41 c0 a8 0a 02 e0 00 . X o @ . . . ^ A . . . .  
0020 00 fb 14 e9 14 e9 00 44 39 f3 00 00 00 00 00 01 . . . . . D 9 . . . .

#: 95 · Time: 19.980787 · Source: 192.168.10.2 · Destination: 224.0.0.251 · Pr... 0x0000 AAAA 5da25e74-fb07-132b-93f7-528468

Show packet bytes Layout: Vertical (Stacked) ▾

6068 146.2229... 192.168.10.2 224.0.0.251 MDNS 102 Standard que

---

### 💡 Question 24:

**What is the upper layer protocol to which this datagram's payload will be delivered?**

📝 Answer:

UDP (17)

📘 Explanation: The Next Header field in IPv6 is 17, indicating UDP.

---

### 💡 Question 25:

**How many IPv6 addresses are returned in the response to this AAAA request?**



**Answer:**  
4 IPv6 addresses



*Explanation:* The DNS response contains 4 AAAA records for youtube.com.

---



### Question 26:

**What is the first IPv6 address returned by the DNS for youtube.com?**



2607:f8b0:4005:805::200e



*Explanation:* This is the smallest (numerically) of the returned addresses.

```
✓ User Datagram Protocol, Src Port: 5555, Dst Port: 53
▼ Multicast Domain Name System (query)
  Transaction ID: 0x0000
  ▶ Flags: 0x0000 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▶ Queries
    [Response In: 287]
```

---