

CS-315 COMPUTER NETWORKS LAB-7 (IP)

PART-1

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the detailed view of packet 230, which is an Internet Protocol Version 4 (IPv4) packet. The packet details are as follows:

- Frame 230: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{...}
- Ethernet II, Src: ChongqingFug_47:3c:11 (c8:94:02:47:3c:11), Dst: Cisco_60:ff:ff (b0:8b:d0:60:ff:ff)
- Internet Protocol Version 4, Src: 10.200.93.33, Dst: 128.119.245.12
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 56
 - Identification: 0x8436 (33846)
 - 000. = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 1
 - Protocol: UDP (17)
 - Header Checksum: 0x5812 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 10.200.93.33
 - Destination Address: 128.119.245.12
- User Datagram Protocol, Src Port: 62000, Dst Port: 33434

The packet bytes pane shows the raw data of the packet, including the IPv4 header and the UDP payload.

1. IP address of my computer = **10.200.93.33**
2. Value of time-to-live(TTL) field = **1**
3. **UDP(17)** is the value in the upper layer protocol field.
4. **20 bytes**(can be seen in the Header Length field)
5. **36 bytes**, since the total length is 56 bytes and the header length is 20 bytes, the payload will be $56 - 20 = 36$ bytes.
6. **No**, the IP datagram has not been fragmented because we can see the flags field is not set, i.e., inside the flags field, the More fragments flag is not set. Also, Fragment Offset = 0.
7. **Header checksum, Time to Live(TTL), and Identification** fields always change from one datagram to another. These fields change

because the traceroute intentionally manipulates them to probe the network path to a destination. Header checksum changes since the header changes for each IP datagram. The identification field is unique for each IP datagram. So, the Identification field value changes. TTL value changes because each packet traceroute sends has an incrementally higher TTL value, allowing it to discover the path packets take to reach the destination and the maximum number of hops required to reach it.

8. **Version, Header Length, Differentiated Services Field, Total Length, Flags, Fragment Offset, Protocol, Source address and Destination address** fields do not change. These fields remain constant because they represent fixed parameters of the communication session or properties of the destination that are unaffected by the traceroute process. Version and Header length does not change since we are using IPv4 and the same protocol for all. The protocol and Services field do not change as we are using the same protocol for all. Source and Destination address are understandably the same. Since there are no fragments, the Flags and Fragment offset will be the same(=zero) for all.
9. The values in the Identification field of the IP datagrams are **sequential**, the value in each subsequent datagram **increases by 1** from the previous one(**serial increment**).
10. Protocol = **ICMP(1)**.
11. For all ICMP packets having the **same source address(same router)**, Yes, the Identification value is in sequential order(serial increment - increasing by 1 from previous ones). Yes, the **behaviour is similar** to that in question 9.
12. No, the values are **not similar** across all of the ICMP packets from all of the routers. Only packets having the same source address(same router) have similar values in the TTL field.

PART-2

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area is divided into three panes. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The bottom-left pane shows the packet details for the selected packet (No. 16), and the bottom-right pane shows the packet bytes in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
13	00:03:35.267568	10.200.93.33	10.250.200.3	DNS	77	Standard query 0x1fd8 AAAA gaia.cs.umass.edu
14	00:03:35.269266	10.250.200.3	10.200.93.33	DNS	77	Standard query response 0x1fd8 AAAA gaia.cs.umass.edu
15	00:03:35.335270	10.250.200.3	10.200.93.33	DNS	93	Standard query response 0xd5c6 A gaia.cs.umass.edu A 128.119.245.12
16	00:03:35.336451	10.200.93.33	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=83dc) [Reassembled in #18]
17	00:03:35.336451	10.200.93.33	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=83dc) [Reassembled in #18]
18	00:03:35.336451	10.200.93.33	128.119.245.12	UDP	54	51521 → 33434 Len=2972
19	00:03:35.336925	10.200.93.33	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=83dd) [Reassembled in #21]
20	00:03:35.336925	10.200.93.33	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=83dd) [Reassembled in #21]
21	00:03:35.336925	10.200.93.33	128.119.245.12	UDP	54	51522 → 33435 Len=2972
22	00:03:35.337333	10.200.93.33	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=83de) [Reassembled in #24]
23	00:03:35.337333	10.200.93.33	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=83de) [Reassembled in #24]
24	00:03:35.337333	10.200.93.33	128.119.245.12	UDP	54	51523 → 33436 Len=2972

Packet 16 details:

- Frame 16: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface
- Ethernet II, Src: ChongqingFug_47:3c:11 (c8:94:02:47:3c:11), Dst: Cisco_60:ff:ff (b0:00:00:00:00:00)
- Internet Protocol Version 4, Src: 10.200.93.33, Dst: 128.119.245.12
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 1500
 - Identification: 0x83dc (33756)
 - 001. = Flags: 0x1, More fragments
 - 0... = Reserved bit: Not set
 - .0... = Don't fragment: Not set
 - .1. = More fragments: Set
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - > Time to Live: 1
 - Protocol: UDP (17)
 - Header Checksum: 0x32c8 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 10.200.93.33
 - Destination Address: 128.119.245.12

Packet bytes (hex and ASCII):

```
0000  b0 8b d0 60 ff ff c8 94 02 47 3c 11 08 00 45 00  ....G<...E-
0010  05 dc 83 dc 20 00 01 11 32 c8 0a c8 5d 21 80 77  ....2...!..w
0020  f5 0c c9 41 82 9a 0b a4 1a f0 40 41 42 43 44 45  ..A....@ABCDE
0030  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
0040  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_abcde
0050  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
0060  76 77 78 79 7a 7b 7c 7d 7e 7f 40 41 42 43 44 45  vwxyz{|}~@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 40 41 42 43 44 45  vwxyz{|}~@ABCDE
00b0  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
00c0  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_abcde
00d0  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
00e0  76 77 78 79 7a 7b 7c 7d 7e 7f 40 41 42 43 44 45  vwxyz{|}~@ABCDE
00f0  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
0100  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_abcde
0110  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
0120  76 77 78 79 7a 7b 7c 7d 7e 7f 40 41 42 43 44 45  vwxyz{|}~@ABCDE
0130  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
0140  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65  VWXYZ[\]^_abcde
0150  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75  fghijklm nopqrstu
0160  76 77 78 79 7a 7b 7c 7d 7e 7f 40 41 42 43 44 45  vwxyz{|}~@ABCDE
```

1. Packet no **16** is the first IP datagram containing the first part of the segment sent to 128.119.245.12 sent by my computer. Packets **16**, **17**, and **18** are three IP datagrams created by fragmenting the first single 3000-byte UDP segment sent to 128.119.145.12. **Yes, the segment has been fragmented** across more than one IP datagram because we can see that the More fragments flag is set.
2. We can see inside the flags field that the **'More fragments' flag field is set(to 1)** which indicates that this datagram has been fragmented.
3. If the **Fragment offset** in the IP header is set to **0(zero)**, it indicates that this is the first fragment. If it is not zero, then it indicates that it is a later fragment.

4. **1500 bytes**, as we can see from the screenshot above in the Total Length field.
5. **Fragment Offset and Header Checksum** are the fields that change in the IP header between the first and second fragment.
6. Packet no **18** is the IP datagram containing the third fragment of the original UDP segment. The **'More fragments' flag field for this packet is not set and the 'Fragment Offset' value is not equal to zero** which indicates that this is the last fragment of that segment.

```

• 16 00:03:35.336451 10.200.93.33 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=83dc) [Reassembled in #18]
• 17 00:03:35.336451 10.200.93.33 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=83dc) [Reassembled in #18]
• 18 00:03:35.336451 10.200.93.33 128.119.245.12 UDP 54 51521 → 33434 Len=2972
19 00:03:35.336925 10.200.93.33 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=83dd) [Reassembled in #21]
20 00:03:35.336925 10.200.93.33 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=83dd) [Reassembled in #21]
21 00:03:35.336925 10.200.93.33 128.119.245.12 UDP 54 51522 → 33435 Len=2972
22 00:03:35.337333 10.200.93.33 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=83de) [Reassembled in #24]
23 00:03:35.337333 10.200.93.33 128.119.245.12 IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=1480, ID=83de) [Reassembled in #24]
24 00:03:35.337333 10.200.93.33 128.119.245.12 UDP 54 51523 → 33436 Len=2972

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x83dc (33756)
v 000. .... = Flags: 0x00
0... .... = Reserved bit: Not set
.0... .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0001 0111 0010 = Fragment Offset: 2960
> Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0x570a [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.200.93.33
Destination Address: 128.119.245.12
> [3 IPv4 Fragments (2980 bytes): #16(1480), #17(1480), #18(20)]
0000 b0 8b d0 60 ff ff c8 94 02 47 3c 11 08 00 45 00 ...G
0010 00 28 83 dc 01 72 01 11 57 0a 0a c8 5d 21 80 77 ...W
0020 f5 0c 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 ...HIJKLM NOI
0030 56 57 58 59 5a 5b ...WXYZ[

```

PART-3

1. Source IPv6 address = **2601:193:8302:4620:215c:f5ae:8b40:a27a**
2. Destination IPv6 address = **2001:558:feed::1**
3. From the below screenshot, we can see the value of the flow label = **0x63ed0**
4. **37 bytes** (can be seen in Payload length field)
5. **UDP(17)** is the upper layer protocol.

No.	Time	Source	Destination	Protocol	Length	Info
12	02:44:45.386940	10.0.0.44	52.114.132.119	TCP	242	[TCP Retransmission] 49987 → 443 [PSH, ACK] Seq=1 Ack=337 Win=4096 Len=188
13	02:44:45.503469	52.114.132.119	10.0.0.44	TCP	60	443 → 49987 [ACK] Seq=337 Ack=189 Win=2051 Len=0
14	02:44:45.525513	52.114.132.119	10.0.0.44	TCP	66	[TCP Dup ACK 13#1] 443 → 49987 [ACK] Seq=337 Ack=189 Win=2051 Len=0 SLE=1 SRE=189
15	02:44:45.698797	10.0.0.123	224.0.0.251	MDNS	139	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _sleep-proxy._u...
16	02:44:45.699096	fe80::1085:6434:358...ff02::fb		MDNS	159	Standard query 0x0000 PTR _companion-link._tcp.local, "QU" question PTR _sleep-proxy._u...
17	02:44:46.313178	Sonos_25:3a:2a	Spanning-tree-for-	STP	60	Conf. Root = 36864/0/48:a6:b8:25:3a:2a Cost = 0 Port = 0x8001
18	02:44:46.675338	52.112.115.23	10.0.0.44	TCP	56	443 → 50518 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	02:44:46.859838	2601:193:8302:4620::...	2001:558:feed::1	DNS	91	Standard query 0x4667 A youtube.com
20	02:44:46.859963	2601:193:8302:4620::...	2001:558:feed::1	DNS	91	Standard query 0x920d AAAA youtube.com
21	02:44:46.864844	2601:193:8302:4620::...	2001:558:feed::1	DNS	95	Standard query 0x7884 A www.youtube.com
22	02:44:46.865379	2601:193:8302:4620::...	2001:558:feed::1	DNS	95	Standard query 0x04fe AAAA www.youtube.com
23	02:44:46.992320	2001:558:feed::1	2601:193:8302:4620::...	DNS	107	Standard query response 0x4667 A youtube.com A 172.217.10.142
24	02:44:46.999326	2001:558:feed::1	2601:193:8302:4620::...	DNS	241	Standard query response 0x04fe AAAA www.youtube.com CNAME youtube-ui.l.google.com AAAA ...
25	02:44:47.000237	2601:193:8302:4620::...	2001:558:feed::1	DNS	103	Standard query 0x7884 A youtube-ui.l.google.com

> Frame 20: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0

> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: VantivaUSA_81:74:5a (44:1c:12:81:74:5a)

> Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Dst: 2001:558:feed::1

0110 = Version: 6

> 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)

.... 0110 0011 1110 0000 = Flow Label: 0x63ed0

Payload Length: 37

Next Header: UDP (17)

Hop Limit: 255

Source Address: 2601:193:8302:4620:215c:f5ae:8b40:a27a

Destination Address: 2001:558:feed::1

6. One IPv6 address is returned in the response(Packet No 27) to this AAAA request.

```

Domain Name System (response)
  Transaction ID: 0x920d
  > Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 0
  > Queries
  > Answers
    > youtube.com: type AAAA, class IN, addr 2607:f8b0:4006:815::200e
      Name: youtube.com
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
      Time to live: 201 (3 minutes, 21 seconds)
      Data length: 16
      AAAA Address: 2607:f8b0:4006:815::200e

```

7. **2607:f8b0:4006:815::200e** is the first of the IPv6 addresses returned by the DNS for youtube.com in the response (packet no. 27) to the DNS AAAA request made in the 20th packet. But, considering all received DNS responses, the first would be **2607:f8b0:4006:806::200e** which is in the DNS response in packet 24 (response to DNS request made in packet no. 22 and not packet no. 20).

```

Answers
  > www.youtube.com: type CNAME, class IN, cname youtube-ui.l.google.com
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:806::200e
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81a::200e
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81b::200e
  > youtube-ui.l.google.com: type AAAA, class IN, addr 2607:f8b0:4006:807::200e

```