

# Assignment 7

## Part-1

udplicmp							
No.	Time	Source	Destination	Protocol	Length	Info	
58	16.628546	10.200.178.190	10.250.200.3	DNS	77	Standard query	0x6884 A gaia.cs.umass.edu
59	16.628889	10.200.178.190	10.250.200.3	DNS	77	Standard query	0xa895 AAAA gaia.cs.umass.edu
65	16.651219	10.250.200.3	10.200.178.190	DNS	93	Standard query response	0x6884 A gaia.cs.umass.edu A 128.119.245.12
69	16.652341	10.250.200.3	10.200.178.190	DNS	77	Standard query response	0xa895 AAAA gaia.cs.umass.edu
70	16.653193	10.200.178.190	10.250.200.3	DNS	77	Standard query	0x9074 AAAA gaia.cs.umass.edu
71	16.655574	10.250.200.3	10.200.178.190	DNS	77	Standard query response	0x9074 AAAA gaia.cs.umass.edu
72	16.657296	10.200.178.190	128.119.245.12	UDP	70	61341 → 33443	Len=28
73	16.657308	10.200.178.190	128.119.245.12	UDP	70	61307 → 33438	Len=28
74	16.657325	10.200.178.190	128.119.245.12	UDP	70	61313 → 33446	Len=28
75	16.657337	10.200.178.190	128.119.245.12	UDP	70	61286 → 33441	Len=28
76	16.657337	10.200.178.190	128.119.245.12	UDP	70	61291 → 33449	Len=28
77	16.657451	10.200.178.190	128.119.245.12	UDP	70	61340 → 33444	Len=28
78	16.657491	10.200.178.190	128.119.245.12	UDP	70	61299 → 33447	Len=28
Internet Protocol Version 4, Src: 10.200.178.190, Dst: 128.119.245.12							
0100 .... = Version: 4				0000 44 b6 be 0a 8f 58 14 13 33 c7 3e 39 08 00 45			
.... 0101 = Header Length: 20 bytes (5)				0010 00 38 a2 16 00 00 03 11 e2 94 0a c8 b2 be 80			
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)				0020 f5 0c ef 9d 82 a3 00 24 20 12 40 41 42 43 44			
Total Length: 56				0030 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54			
Identification: 0xa216 (41494)				0040 56 57 58 59 5a 5b			
> 000. .... = Flags: 0x0							
...0 0000 0000 0000 = Fragment Offset: 0							
> Time to Live: 3							
Protocol: UDP (17)							
Header Checksum: 0xe294 [validation disabled]							
[Header checksum status: Unverified]							
Source Address: 10.200.178.190							
Destination Address: 128.119.245.12							
> User Datagram Protocol, Src Port: 61341, Dst Port: 33443							

1. The IP address of my computer is: **10.200.178.190**
2. The time-to-live (TTL) value is: **3**
3. The value in the upper layer protocol field in this IPv4 datagram's header is: **UDP**
4. There are **20 bytes** in the IP header
5. The total length of the IP datagram is 56 bytes and the header length is 20 bytes. Therefore to calculate the length of payload of the IP datagram we subtract header length from total length. Hence,  
Length of payload = (Total Length - Header Length)  
= 56 - 20  
= **36**
6. **No**, the IP datagram is not fragmented as the Fragment Offset is **0**
7. Fields in the IP datagram that always change from one datagram to the next are:  
**Identification** (because IP packets must have different IDs)  
**Time to Live** (because Traceroute increments each subsequent packet)  
**Header Checksum** (Reason: As the header changes, so the checksum should also change)
8. The fields that stay(and must stay) constant across the IP datagrams are:  
**Version** (since we are using IPv4 for all packets)  
**Header Length** (since these are ICMP packets)  
**Source IP** (since we are sending from the same source)  
**Destination IP** (since we are sending to the same dest)  
**Differentiated Services** (since all packets are ICMP they use the same Type of Service class)  
**Upper Layer Protocol** (since these are ICMP packets)

9. With each ICMP Echo (ping) request, the IP header Identification field displays a random integer value.
10. The value in the upper layer protocol field in this IPv4 datagram's header is: **ICMP (1)**
11. **Yes**, The Identification fields change the values across the sequence of all ICMP packets from all of the routers.
12. **No**, the values of TTL fields also change across all of the ICMP packets from all of the routers.

## Part-2

483	40.41067...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=bd75) [Reassembled in #485]
484	40.41068...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=bd75) [Reassembled in #485]
485	40.41068...	10.240.118.72	128.119.245.12	UDP	54	59666 → 33434 Len=2972
486	40.41071...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0211) [Reassembled in #488]
487	40.41071...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0211) [Reassembled in #488]
488	40.41071...	10.240.118.72	128.119.245.12	UDP	54	35673 → 33435 Len=2972
489	40.41073...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b5c8) [Reassembled in #491]
490	40.41073...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b5c8) [Reassembled in #491]

  

```

> Frame 484: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on inter
> Ethernet II, Src: HP_0a:79:b1 (e0:73:e7:0a:79:b1), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2
  > Internet Protocol Version 4, Src: 10.240.118.72, 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: 0xbd75 (48501)
    > 001. .... = Flags: 0x1, More fragments
      0... .... = Reserved bit: Not set
      .0... .... = Don't fragment: Not set
      ..1. .... = More fragments: Set
      ...0 0000 1011 0001 = Fragment Offset: 1480
    > Time to Live: 1
    Protocol: UDP (17)
  
```

0000	f8 7a 41 13 2a c2 e0 73	e7 0a 79 b1 08 00 45 00	~Z~*
0010	05 dc bd 75 20 b9 01 11	df 26 0a f0 76 48 80 77	~..u
0020	f5 0c 40 41 42 43 44 45	46 47 48 49 4a 4b 4c 4d	~@AB
0030	4e 4f 50 51 52 53 54 55	56 57 58 59 5a 5b 5c 5d	NOPQR
0040	5e 5f 60 61 62 63 64 65	66 67 68 69 6a 6b 6c 6d	^_`ab
0050	6e 6f 70 71 72 73 74 75	76 77 78 79 7a 7b 7c 7d	nopqr
0060	7e 7f 40 41 42 43 44 45	46 47 48 49 4a 4b 4c 4d	~@AB
0070	4e 4f 50 51 52 53 54 55	56 57 58 59 5a 5b 5c 5d	NOPQR
0080	5e 5f 60 61 62 63 64 65	66 67 68 69 6a 6b 6c 6d	^_`ab
0090	6e 6f 70 71 72 73 74 75	76 77 78 79 7a 7b 7c 7d	nopqr
00a0	7e 7f 40 41 42 43 44 45	46 47 48 49 4a 4b 4c 4d	~@AB
00b0	4e 4f 50 51 52 53 54 55	56 57 58 59 5a 5b 5c 5d	NOPQR
00c0	5e 5f 60 61 62 63 64 65	66 67 68 69 6a 6b 6c 6d	^_`ab
00d0	6e 6f 70 71 72 73 74 75	76 77 78 79 7a 7b 7c 7d	nopqr
00e0	7e 7f 40 41 42 43 44 45	46 47 48 49 4a 4b 4c 4d	~@AB
00f0	4e 4f 50 51 52 53 54 55	56 57 58 59 5a 5b 5c 5d	NOPQR
0100	5e 5f 60 61 62 63 64 65	66 67 68 69 6a 6b 6c 6d	^_`ab
0110	6e 6f 70 71 72 73 74 75	76 77 78 79 7a 7b 7c 7d	nopqr

1. **Yes**, The segment has been fragmented across more than one IP datagram
2. The **More Fragments offset** within the flags header in IP header indicates that the datagram has been fragmented or not.
3. Since the **fragment offset is 0**, we know that this is the first fragment.
4. There are **1500 bytes** (Header Length + Payload) in this IP datagram.
5. The fields that change in the IP header between the first and second fragment are:

- **Fragment Offset**
- **Header Checksum**

483	40.41067...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=bd75) [Reassembled in #485]
484	40.41068...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=bd75) [Reassembled in #485]
485	40.41068...	10.240.118.72	128.119.245.12	UDP	54	59666 → 33434 Len=2972
486	40.41071...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0211) [Reassembled in #488]
487	40.41071...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=0211) [Reassembled in #488]
488	40.41071...	10.240.118.72	128.119.245.12	UDP	54	35673 → 33435 Len=2972
489	40.41073...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=b5c8) [Reassembled in #491]
490	40.41073...	10.240.118.72	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=1480, ID=b5c8) [Reassembled in #491]

  

```

> Frame 485: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eno
> Ethernet II, Src: HP_0a:79:b1 (e0:73:e7:0a:79:b1), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2
  > Internet Protocol Version 4, Src: 10.240.118.72, 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: 40
      Identification: 0xbd75 (48501)
    > 000. .... = Flags: 0x0
      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)
  
```

0000	f8 7a 41 13 2a c2 e0 73	e7 0a 79 b1 08 00 45 00	~Z~*
0010	00 28 bd 75 01 72 01 11	04 22 0a f0 76 48 80 77	~(.u
0020	f5 0c 48 49 4a 4b 4c 4d	4e 4f 50 51 52 53 54 55	~HIJ
0030	56 57 58 59 5a 5b		VWXYZ

### Part-3

```
> Frame 20: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface en0, id 0000
> Ethernet II, Src: Apple_98:d9:27 (78:4f:43:98:d9:27), Dst: VantivaUSA_81:74:5a (44:1c:1d:00:00:00)
> Internet Protocol Version 6, Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Dst: 2001:558:0000:0000:0000:0000:0000:0000
    0110 .... = Version: 6
    > .... 0000 0000 .... .. = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECN)
    .... 0110 0011 1110 1101 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
> User Datagram Protocol, Src Port: 64430, Dst Port: 53
> Domain Name System (query)
```

No.	Time	Source	Destination	Protocol	Length	Info
16	2.653622	fe80::1085:6434:358...	ff02::fb	MDNS	159	Standard query 0x0000 PTR _companion-link_tcp.local, "QU" question PTR _sleep-proxy_udp.local.
17	3.267704	Sonos_25:3a:2a	Spanning-tree-for...	STP	60	Conf. Root = 36864/0/48:a6:b8:25:3a:2a Cost = 0 Port = 0x8001
18	3.629864	52.112.115.23	10.0.0.44	TCP	56	443 → 50518 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19	3.814364	2601:193:8302:4620::	2001:558:feed::1	DNS	91	Standard query 0x4667 A youtube.com
20	3.814489	2601:193:8302:4620::	2001:558:feed::1	DNS	91	Standard query 0x92d0 AAAA youtube.com
21	3.819370	2601:193:8302:4620::	2001:558:feed::1	DNS	95	Standard query 0x7884 A www.youtube.com
22	3.819905	2601:193:8302:4620::	2001:558:feed::1	DNS	95	Standard query 0x04fe AAAA www.youtube.com
23	3.946846	2001:558:feed::1	2601:193:8302:4620::	DNS	107	Standard query response 0x4667 A youtube.com A 172.217.10.142
24	3.953852	2001:558:feed::1	2601:193:8302:4620::	DNS	241	Standard query response 0x04fe AAAA www.youtube.com CNAME youtube-ui-1.google.com AAAA 2607:f8b...
25	3.954763	2601:193:8302:4620::	2001:558:feed::1	DNS	103	Standard query 0x7884 A youtube-ui-1.google.com

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

> User Datagram Protocol, Src Port: 53, Dst Port: 57174

▼ Domain Name System (response)

Transaction ID: 0x04fe

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 5

Authority RRs: 0

Additional RRs: 0

> Queries

▼ Answers

> www.youtube.com: type CNAME, class IN, cname youtube-ui-1.google.com

> youtube-ui-1.google.com: type AAAA, class IN, addr 2607:f8b0:4006:806::200e

> youtube-ui-1.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81a::200e

> youtube-ui-1.google.com: type AAAA, class IN, addr 2607:f8b0:4006:81b::200e

> youtube-ui-1.google.com: type AAAA, class IN, addr 2607:f8b0:4006:807::200e

[Request In: 22]

[Time: 0.133947000 seconds]

```

0000  78 4f 43 98 d9 27 44 c1 12 81 74 5a 86 dd 60 00  xOC'D'..tZ..
0010  00 00 00 bb 11 3a 20 01 05 58 fe ed 00 00 00 00  .....X.....
0020  00 00 00 00 01 26 01 01 93 83 02 46 20 21 5c    .....f\|
0030  f5 ae 8b 40 a2 7a 00 35 df 56 00 bb 8c 03 04 fe  @z5-V.....
0040  81 80 00 01 00 05 00 00 00 03 77 77 77 07 79    .....www.y
0050  6f 75 74 75 62 65 03 63 6f 6d 00 00 1c 00 01 c  outube.c om...
0060  0c 00 05 00 00 b2 00 00 16 0a 79 6f 75 74      .....yout
0070  75 62 65 2d 75 69 01 6c 06 6f 6f 6f 6c 65 c0  ube-ui.l google
0080  18 c0 2d 00 1c 01 00 00 00 c1 00 10 26 07 f8    .....&...
0090  b0 40 06 8b 06 00 00 00 00 00 20 0e c0 2d 00  @.....
00a0  1c 00 01 00 00 00 c1 00 10 26 07 f8 b0 40 06 08  &.....@
00b0  1a 00 00 00 00 00 20 0e c0 2d 00 1c 00 01 00  @.....
00c0  00 00 c1 00 10 26 07 f8 b0 40 06 8b 10 00 00 00  &.....@
00d0  00 00 00 20 0e c0 2d 00 1c 00 01 00 00 c1 00  @.....
00e0  10 26 07 f8 b0 40 06 08 07 00 00 00 00 00 00 20  &.....@
00f0  0e

```

1. The IPv6 address of the computer making the DNS AAAA request is: **2601:193:8302:4620:215c:f5ae:8b40:a27a**
2. The IPv6 destination address for this datagram is: **2001:558:feed::1**
3. The value of the flow label for this datagram is: **0x063ed0**
4. The payload has **37 bytes** of data carried in it.
5. The upper layer protocol to which the datagram's payload will be delivered is: **UDP (17)**
6. **4** IPv6 addresses are returned in the response to this AAAA request.
7. The first of the IPv6 addresses returned by the DNS for youtube.com is:  
**2607:f8b0:4006:806::200e**