

Wireshark Lab: IP

- Source Address: 144.122.149.172
- Time to Live: 1
- Protocol: UDP (17)
- Header Length: 20 bytes
- Total Length: 56 - Header: 20 bytes = 36 bytes
- More fragments: Not set, and Fragment Offset: 0, so It is not fragmented.

No.	Time	Source	Destination	Protocol	Length	Info
109	3.420494	144.122.149.172	128.119.245.12	UDP	70	39033 → 33435 Len=28
110	3.423530	144.122.149.172	128.119.245.12	UDP	70	39033 → 33435 Len=28
111	3.424887	144.122.149.172	128.119.245.12	UDP	70	39033 → 33437 Len=28
112	3.426881	144.122.149.172	128.119.245.12	UDP	70	39033 → 33438 Len=28
113	3.428984	144.122.149.172	128.119.245.12	UDP	70	39033 → 33439 Len=28
114	3.430528	144.122.149.172	128.119.245.12	UDP	70	39033 → 33440 Len=28
115	3.432722	144.122.149.172	128.119.245.12	UDP	70	39033 → 33441 Len=28
116	3.434991	144.122.149.172	128.119.245.12	UDP	70	39033 → 33442 Len=28
117	3.437199	144.122.149.172	128.119.245.12	UDP	70	39033 → 33443 Len=28

```

> Frame 105: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Apple_23:4c:62 (94:f6:d6:23:4c:62), Dst: Intel_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.149.172, 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: 0x987a (39034)
  > 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    > [Expert Info (Note/Sequence): "Time to Live" only 1]
    Protocol: UDP (17)
    Header Checksum: 0x8590 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 144.122.149.172
    Destination Address: 128.119.245.12
  > User Datagram Protocol, Src Port: 39033, Dst Port: 33435
    Source Port: 39033
    Destination Port: 33435
    > [Expert Info (Chat/Sequence): Possible traceroute: hop #1, attempt #1]
    Length: 36
    Checksum: 0x48e6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 44]
    > [Timestamps]
    UDP payload (28 bytes)
    > Data (28 bytes)

```

No.	Time	Source	Destination	Protocol	Length	Info
105	3.416218	144.122.149.172	128.119.245.12	UDP	70	39033 → 33435 Len=28
110	3.423530	144.122.149.172	128.119.245.12	UDP	70	39033 → 33436 Len=28
113	3.424887	144.122.149.172	128.119.245.12	UDP	70	39033 → 33437 Len=28
115	3.426881	144.122.149.172	128.119.245.12	UDP	70	39033 → 33438 Len=28
117	3.428984	144.122.149.172	128.119.245.12	UDP	70	39033 → 33439 Len=28
119	3.430528	144.122.149.172	128.119.245.12	UDP	70	39033 → 33440 Len=28
121	3.432722	144.122.149.172	128.119.245.12	UDP	70	39033 → 33441 Len=28
257	8.441991	144.122.149.172	128.119.245.12	UDP	70	39033 → 33442 Len=28
318	8.441991	144.122.149.172	128.119.245.12	UDP	70	39033 → 33443 Len=28

```

> Frame 105: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Apple_23:4c:62 (94:f6:d6:23:4c:62), Dst: Intel_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.149.172, 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: 0x987a (39034)
  > 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    > [Expert Info (Note/Sequence): "Time to Live" only 1]
    Protocol: UDP (17)
    Header Checksum: 0x8590 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 144.122.149.172
    Destination Address: 128.119.245.12
  > User Datagram Protocol, Src Port: 39033, Dst Port: 33435
    Source Port: 39033
    Destination Port: 33435
    > [Expert Info (Chat/Sequence): Possible traceroute: hop #1, attempt #1]
    Length: 36
    Checksum: 0x48e6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 44]
    > [Timestamps]
    UDP payload (28 bytes)
    > Data (28 bytes)

```

No.	Time	Source	Destination	Protocol	Length	Info
121	3.430772	144.122.149.172	128.119.245.12	UDP	70	39033 → 33441 Len=28
257	8.441991	144.122.149.172	128.119.245.12	UDP	70	39033 → 33442 Len=28
360	11.4471..	144.122.149.172	128.119.245.12	UDP	70	39033 → 33443 Len=28
441	18.4523..	144.122.149.172	128.119.245.12	UDP	70	39033 → 33444 Len=28
443	18.4536..	144.122.149.172	128.119.245.12	UDP	70	39033 → 33445 Len=28
447	18.4671..	144.122.149.172	128.119.245.12	UDP	70	39033 → 33447 Len=28
449	18.4703..	144.122.149.172	128.119.245.12	UDP	70	39033 → 33448 Len=28

```

> Frame 445: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Apple_23:4c:62 (94:f6:d6:23:4c:62), Dst: Intel_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.149.172, 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: 0x9885 (39045)
  > 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 4
    > [Expert Info (Note/Sequence): "Time to Live" only 4]
    Protocol: UDP (17)
    Header Checksum: 0x8285 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 144.122.149.172
    Destination Address: 128.119.245.12
  > User Datagram Protocol, Src Port: 39033, Dst Port: 33446
    Source Port: 39033
    Destination Port: 33446
    > [Expert Info (Chat/Sequence): Possible traceroute: hop #1, attempt #1]
    Length: 36
    Checksum: 0x48e6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 44]
    > [Timestamps]
    UDP payload (28 bytes)
    > Data (28 bytes)

```

- The header checksum and the Identification always change from one datagram to the next. The header checksum changes because the header changes, identification changes to verify different packets
- Version(IPv4), Length of header (because it is fixed for all), Source IP(because of sending from same place), Destination IP(because of sending to same place), Upper layer protocol(always uses UDP)
- Increases by one for the next packet

No.	Time	Source	Destination	Protocol	Length	Info
109	3.420494	144.122.148.1	144.122.149.172	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
112	3.423743	144.122.148.1	144.122.149.172	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
114	3.425747	144.122.148.1	144.122.149.172	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
116	3.428006	144.122.2.1	144.122.149.172	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
118	3.432275	144.122.2.1	144.122.149.172	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
120	3.436544	144.122.2.1	144.122.149.172	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
442	18.4571..	193.140.85.137	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
444	18.4631..	193.140.85.137	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
446	18.4693..	193.140.85.137	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
448	18.4782..	193.140.8.150	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
450	18.4898..	193.140.8.150	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
452	18.5016..	193.140.8.150	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
454	18.5085..	62.40.125.129	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
458	18.5608..	62.40.125.129	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
460	18.5931..	62.40.125.129	144.122.149.172	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
462	18.6477..	62.40.98.45	144.122.149.172	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
464	18.7051..	62.40.98.45	144.122.149.172	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
470	18.7613..	62.40.98.45	144.122.149.172	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
472	18.8166..	62.40.98.242	144.122.149.172	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
476	18.8723..	62.40.98.242	144.122.149.172	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
478	18.9280..	62.40.98.242	144.122.149.172	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

- Protocol: ICMP (1)
- No, they are not increased by one as it was in 9th question, they are different.
- No, they are not similar, they change