ICMP

ICMP (Internet Control Message Protocol) - It is a protocol which is used for reachability, troubleshooting and network management. ICMP mainly used in Ping Utility Protocol Ping uses ICMP Request & Reply for its process. If any source is not reachable, ICMP sends an error message to source.

Types of ICMP packet

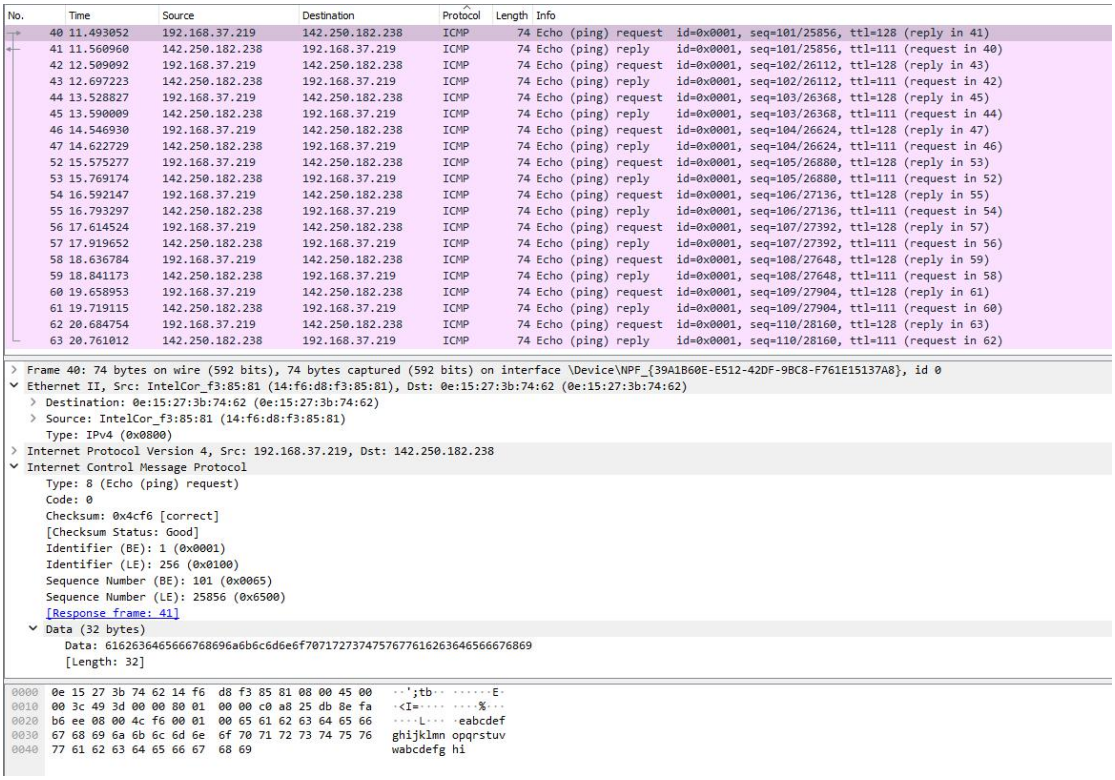
- 8 - ICMP Request
- 0 - ICMP Reply
- 3 - Destination Unreachable
  - 0 - Destination network unreachable
  - 1 - Destination host unreachable
  - 13 - Packet administratively Filtered Checksum - Correct or not
- 11 - Time to live exceeded

Creating Ping request and analyzing using WireShark

```
PS C:\Users\Sceke> ping -n 10 youtube.in

Pinging youtube.in [142.250.182.238] with 32 bytes of data:
Reply from 142.250.182.238: bytes=32 time=68ms TTL=111
Reply from 142.250.182.238: bytes=32 time=188ms TTL=111
Reply from 142.250.182.238: bytes=32 time=61ms TTL=111
Reply from 142.250.182.238: bytes=32 time=76ms TTL=111
Reply from 142.250.182.238: bytes=32 time=194ms TTL=111
Reply from 142.250.182.238: bytes=32 time=201ms TTL=111
Reply from 142.250.182.238: bytes=32 time=305ms TTL=111
Reply from 142.250.182.238: bytes=32 time=204ms TTL=111
Reply from 142.250.182.238: bytes=32 time=60ms TTL=111
Reply from 142.250.182.238: bytes=32 time=76ms TTL=111

Ping statistics for 142.250.182.238:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 305ms, Average = 143ms
```



No.	Time	Source	Destination	Protocol	Length	Info
40	11.493052	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=101/25856, ttl=128 (reply in 41)
41	11.560960	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=101/25856, ttl=111 (request in 40)
42	12.509092	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (reply in 43)
43	12.697223	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=102/26112, ttl=111 (request in 42)
44	13.528827	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=103/26368, ttl=128 (reply in 45)
45	13.590009	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=103/26368, ttl=111 (request in 44)
46	14.546930	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=104/26624, ttl=128 (reply in 47)
47	14.622729	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=104/26624, ttl=111 (request in 46)
52	15.575277	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=105/26880, ttl=128 (reply in 53)
53	15.769174	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=105/26880, ttl=111 (request in 52)
54	16.592147	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=106/27136, ttl=128 (reply in 55)
55	16.793297	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=106/27136, ttl=111 (request in 54)
56	17.614524	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=107/27392, ttl=128 (reply in 57)
57	17.919652	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=107/27392, ttl=111 (request in 56)
58	18.636784	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=108/27648, ttl=128 (reply in 59)
59	18.841173	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=108/27648, ttl=111 (request in 58)
60	19.658953	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=109/27904, ttl=128 (reply in 61)
61	19.719115	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=109/27904, ttl=111 (request in 60)
62	20.684754	192.168.37.219	142.250.182.238	ICMP	74	Echo (ping) request id=0x0001, seq=110/28160, ttl=128 (reply in 63)
63	20.761012	142.250.182.238	192.168.37.219	ICMP	74	Echo (ping) reply id=0x0001, seq=110/28160, ttl=111 (request in 62)

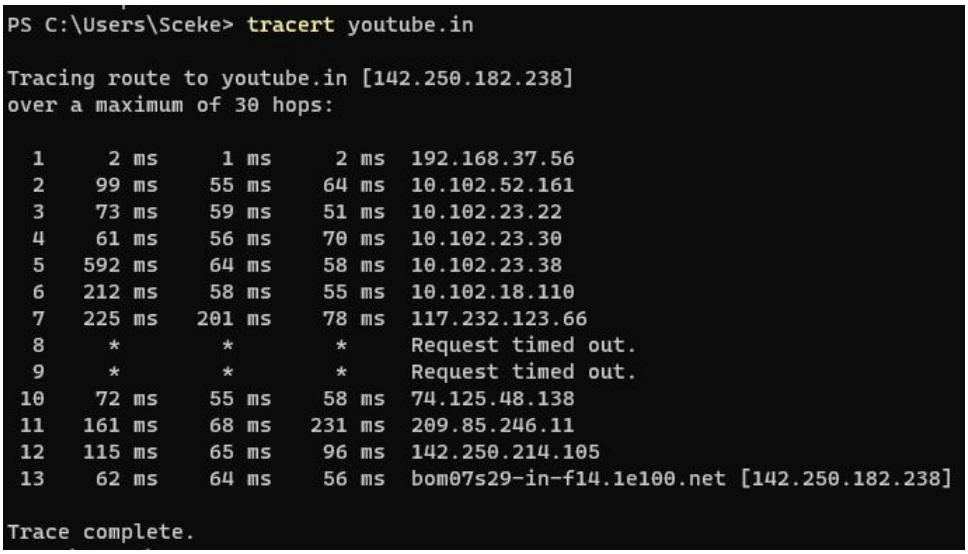
```
> Frame 40: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{39A1B60E-E512-42DF-9BC8-F761E15137A8}, id 0
v Ethernet II, Src: IntelCor_f3:85:81 (14:f6:d8:f3:85:81), Dst: 0e:15:27:3b:74:62 (0e:15:27:3b:74:62)
  > Destination: 0e:15:27:3b:74:62 (0e:15:27:3b:74:62)
  > Source: IntelCor_f3:85:81 (14:f6:d8:f3:85:81)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.37.219, Dst: 142.250.182.238
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cf6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 101 (0x0065)
    Sequence Number (LE): 25856 (0x6500)
    [Response frame: 41]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  0e 15 27 3b 74 62 14 f6  d8 f3 85 81 08 00 45 00   ··';tb·· ·····E·
0010  00 3c 49 3d 00 00 80 01  00 00 c0 a8 25 db 8e fa   ·<I=···· ····%···
0020  b6 ee 08 00 4c f6 00 01  00 65 61 62 63 64 65 66   ····L··· ·eabcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

Tracert

It is used to trace the route from source to destination

- In linux tracert uses UDP protocol
- In windows, it uses ICMP protocol to trace route



UDP (User Datagram Protocol)

UDP is a protocol for transmitting data where there is requirement of Low Latency Transmission. It is assumed to be faster than a TCP connection. It formally doesn't make connection before transmitting data. UDP is faster bit less reliable than TCP Why UDP when we have TCP ? In TCP Handshake,

Step 1: In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.

Step 2: In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.

Step 3: In this final step, the client acknowledges the response of the Server, and they both create a stable connection that will begin the actual data transfer process.

TCP communications indicate the order in which data packets should be received and confirm that packets arrive as intended. If a packet does not arrive, TCP requires that it be re-sent. UDP communications do not include any of this functionality.

Because UDP doesn't need a handshake, or doesn't need to check whther data had been recieved properly or not, due to this the transmission in UDP is much faster than TCP.

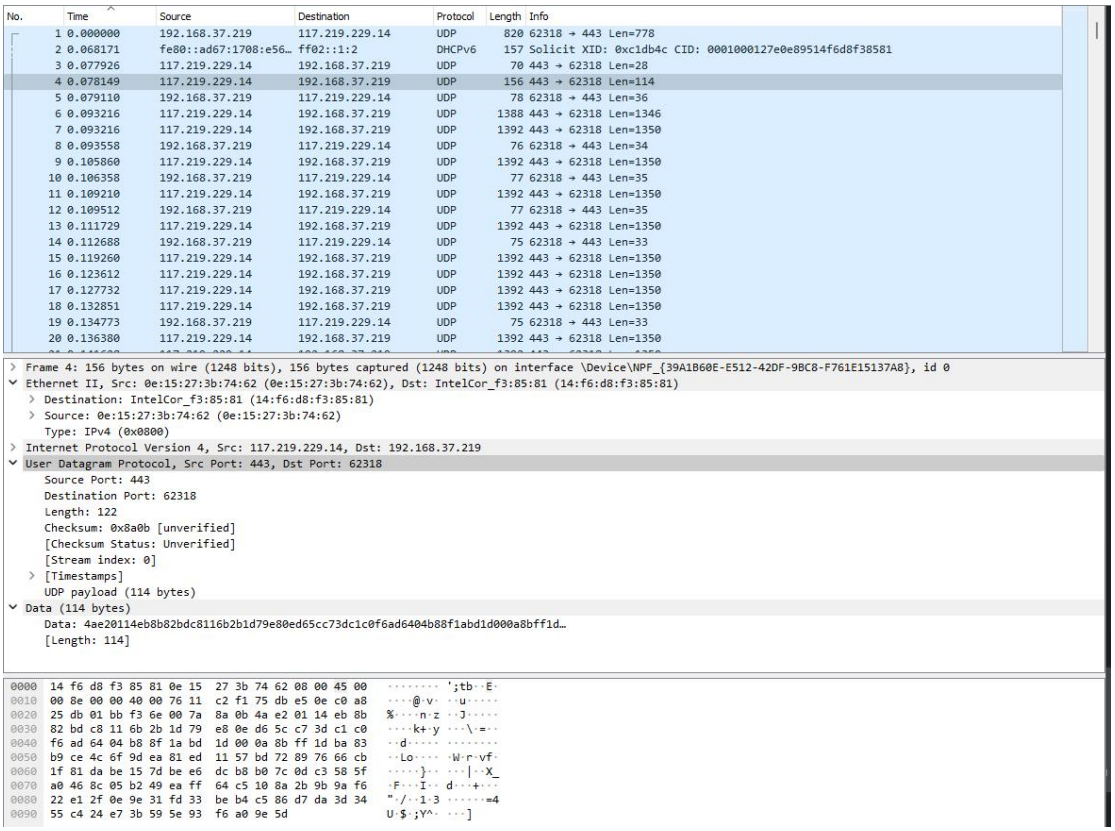
Hence there is tradeoff, if data got lost in between then it will not be re-send again. Hence applications should be loss-tolerant.

It is mostly used in those applications where sometimes dropping packets is more beneficial than waiting for it to retransmit.

Hence, voice & video traffic is sent through this protocol. Even VoIP uses UDP for transmission.

WireShark Analysis:

Youtube live uses UDP so I turn on Youtube live and captured packet using wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.37.219	117.219.229.14	UDP	820	62318 → 443 Len=778
2	0.068171	fe80::ad67:1708:e56…	ff02::1:2	DHCPv6	157	Solicit XID: 0xc1db4c CID: 0001000127e0e89514f6d8f38581
3	0.077926	117.219.229.14	192.168.37.219	UDP	70	443 → 62318 Len=28
4	0.078149	117.219.229.14	192.168.37.219	UDP	156	443 → 62318 Len=114
5	0.079110	192.168.37.219	117.219.229.14	UDP	78	62318 → 443 Len=36
6	0.093216	117.219.229.14	192.168.37.219	UDP	1388	443 → 62318 Len=1346
7	0.093216	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
8	0.093558	192.168.37.219	117.219.229.14	UDP	76	62318 → 443 Len=34
9	0.105860	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
10	0.106358	192.168.37.219	117.219.229.14	UDP	77	62318 → 443 Len=35
11	0.109210	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
12	0.109512	192.168.37.219	117.219.229.14	UDP	77	62318 → 443 Len=35
13	0.111729	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
14	0.112688	192.168.37.219	117.219.229.14	UDP	75	62318 → 443 Len=33
15	0.119260	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
16	0.123612	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
17	0.127732	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
18	0.132851	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350
19	0.134773	192.168.37.219	117.219.229.14	UDP	75	62318 → 443 Len=33
20	0.136380	117.219.229.14	192.168.37.219	UDP	1392	443 → 62318 Len=1350

```
> Frame 4: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface \Device\NPF_{39A1B60E-E512-42DF-9BC8-F761E15137A8}, id 0
v Ethernet II, Src: 0e:15:27:3b:74:62 (0e:15:27:3b:74:62), Dst: IntelCor_f3:85:81 (14:f6:d8:f3:85:81)
  > Destination: IntelCor_f3:85:81 (14:f6:d8:f3:85:81)
  > Source: 0e:15:27:3b:74:62 (0e:15:27:3b:74:62)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 117.219.229.14, Dst: 192.168.37.219
v User Datagram Protocol, Src Port: 443, Dst Port: 62318
    Source Port: 443
    Destination Port: 62318
    Length: 122
    Checksum: 0x8a0b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (114 bytes)
v Data (114 bytes)
    Data: 4ae20114eb8b82bdc8116b2b1d79e80ed65cc73dc1c0f6ad6404b88f1abd1d000a8bff1d…
    [Length: 114]
```

```
0000  14 f6 d8 f3 85 81 0e 15  27 3b 74 62 08 00 45 00   ........ ';tb..E.
0010  00 8e 00 00 40 00 76 11  c2 f1 75 db e5 0e c0 a8   ....@.v. ..u.....
0020  25 db 01 bb f3 6e 00 7a  8a 0b 4a e2 01 14 eb 8b   %....n.z ..J.....
0030  82 bd c8 11 6b 2b 1d 79  e8 0e d6 5c c7 3d c1 c0   ....k+.y ...\.=..
0040  f6 ad 64 04 b8 8f 1a bd  1d 00 0a 8b ff 1d ba 83   ..d..... ........
0050  b9 ce 4c 6f 9d ea 81 ed  11 57 bd 72 89 76 66 cb   ..Lo.... .W.r.vf.
0060  1f 81 da be 15 7d be e6  dc b8 b0 7c 0d c3 58 5f   .....}.. ...|..X_
0070  a0 46 8c 05 b2 49 ea ff  64 c5 10 8a 2b 9b 9a f6   .F...I.. d...+...
0080  22 e1 2f 0e 9e 31 fd 33  be b4 c5 86 d7 da 3d 34   "./..1.3 ......=4
0090  55 c4 24 e7 3b 59 5e 93  f6 a0 9e 5d               U.$.;Y^. ...]
```