

# COMP 3203 Wireshark 9

Name: Nirmith Victor D'Almeida

Number: 101160124

1. The IP address of host is 192.168.1.101. IP address of the source is 143.89.14.34.
2. Since they are designed to communicate network layer information between hosts and routers and not between application layer processes.

3. The ICMP type number is 8 and code is 0

The other fields present are Checksum, Identifier, Sequence Number and Data fields.

They are each 2 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply

> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG\_da:af:73 (00:0c:29:14:af:73)

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 143.89.14.34

▼ Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0xe45a [correct]

[Checksum Status: Good]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 26369 (0x6701)

Sequence Number (LE): 359 (0x0167)

[\[Response frame: 4\]](#)

▼ Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

4. Type is 0 and code is 0.

It contains checksum, Identifier, Sequence number and Data.

The checksum, sequence number and identifier fields are 2 bytes each respectively.

Time	Source	Destination	Protocol	Length	Info
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74 Echo (ping) reply

> Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

> Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)

> Internet Protocol Version 4, Src: 143.89.14.34, Dst: 192.168.1.101

▼ Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xec5a [correct]

[Checksum Status: Good]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 26369 (0x6701)

Sequence Number (LE): 359 (0x0167)

[\[Request frame: 3\]](#)

[Response time: 413.442 ms]

▼ Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

5. IP Address of the host is 192.168.1.101

Target destination is 138.96.146.2

6. Instead of 01 it would be switched to 0 X 11.

7. They are the same as that of the first half of the lab

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded
3	0.013258	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request
4	0.025551	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded

> Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0

> Ethernet II, Src: Dell\_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG\_da:af:73 (08:00:27:08:00:27)

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2

> Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x51fe [correct]

[Checksum Status: Good]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 41985 (0xa401)

Sequence Number (LE): 420 (0x01a4)

> [No response seen]

> Data (64 bytes)

8. They include the IP header as well.

No.	Time	Source	Destination	Protocol	Length	Info
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded
3	0.013258	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0

> Ethernet II, Src: LinksysG\_da:af:73 (00:06:25:da:af:73), Dst: Dell\_4f:36:23 (00:08:74:4f:36:23)

> Internet Protocol Version 4, Src: 10.216.228.1, Dst: 192.168.1.101

> Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Checksum: 0x2c16 [correct]

[Checksum Status: Good]

Unused: 00000000

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2

> Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x51fe [unverified] [in ICMP error packet]

[Checksum Status: Unverified]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 41985 (0xa401)

Sequence Number (LE): 420 (0x01a4)

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 c0 ..tO6#..%..s..E.

0010 00 38 9d 45 00 00 ff 01 6c d8 0a d8 e4 01 c0 a8 .8.E....1.....

0020 01 65 0b 00 2c 16 00 00 00 00 45 00 00 5c d2 d5 .e.,...E..\...

0030 00 00 01 01 d1 45 c0 a8 01 65 8a 60 92 02 08 00 .....E...e`....

0040 51 fe 02 00 a4 01 Q.....

9. Their Message type is 0 rather than 11 from the TTL expired.  
the main reason is because they made it all the way to the destination within the Time to live period.

```

98 18.007202 138.96.146.2 192.168.1.101 ICMP 106 Echo (ping) rep
>
Frame 98: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:
Internet Protocol Version 4, Src: 138.96.146.2, Dst: 192.168.1.101
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x29fe [correct]
  [Checksum Status: Good]
  Identifier (BE): 512 (0x0200)
  Identifier (LE): 2 (0x0002)
  Sequence Number (BE): 54273 (0xd401)
  Sequence Number (LE): 468 (0x01d4)
  [Request frame: 97]
  [Response time: 113.456 ms]
  Data (64 bytes)
96 17.006427 193.51.181.137 192.168.1.101 ICMP 70 Time-to-live ex
<
> Frame 96: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:
> Internet Protocol Version 4, Src: 193.51.181.137, Dst: 192.168.1.101
v Internet Control Message Protocol
  Type: 11 (Time-to-live exceeded)
  Code: 0 (Time to live exceeded in transit)
  Checksum: 0x2c16 [correct]
  [Checksum Status: Good]
  Unused: 00000000
  Internet Protocol Version 4, Src: 192.168.1.101, Dst: 138.96.146.2
v Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x22fe [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier (BE): 512 (0x0200)
  Identifier (LE): 2 (0x0002)
  Sequence Number (BE): 54017 (0xd301)
  Sequence Number (LE): 467 (0x01d3)

```

10. There is a significant delay between step 9 and 10 as seen in the ss of figure 4  
Whereas in my ss (the black one) we can see it from step 11 and 12  
For figure 4 the link is New York City or nyc open transit and Pastourelle opentransit

```
C:\Users\nirmi>tracert www.inria.fr
```

```
Tracing route to inria.fr [128.93.162.83]  
over a maximum of 30 hops:
```

1	3 ms	3 ms	3 ms	mynetwork [192.168.2.1]
2	9 ms	10 ms	13 ms	10.11.3.89
3	*	*	*	Request timed out.
4	10 ms	10 ms	10 ms	dis33-ottawa23_ae3.net.bell.ca [64.230.52.63]
5	*	*	*	Request timed out.
6	*	*	*	Request timed out.
7	27 ms	28 ms	26 ms	cr01-toroon2147w-bundle-ether9.net.bell.ca [142.124.127.118]
8	*	*	*	Request timed out.
9	28 ms	38 ms	30 ms	tc0re3-chicagocp-bundle-ether15.net.bell.ca [142.124.127.96]
10	27 ms	30 ms	27 ms	bx10-chicagodt_ae0.net.bell.ca [64.230.78.173]
11	65 ms	28 ms	26 ms	bx10-chicagodt_et-8/1/2_ae8.net.bell.ca [184.150.181.36]
12	119 ms	121 ms	119 ms	et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
13	118 ms	115 ms	116 ms	renater-gw-ix1.gtt.net [77.67.123.206]
14	116 ms	117 ms	118 ms	te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
15	119 ms	119 ms	119 ms	inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
16	121 ms	118 ms	118 ms	unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
17	119 ms	120 ms	120 ms	prod-inriafr-cms.inria.fr [128.93.162.83]

```
Trace complete.
```

```
Command Prompt
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:

 1  13 ms  12 ms  13 ms  10.216.228.1
 2  21 ms  14 ms  13 ms  24.218.0.153
 3  12 ms  11 ms  13 ms  bar01-p4-0.usfdhe1.ma.attbb.net [24.128.190.197]
 4  16 ms  16 ms  15 ms  bar02-p6-0.ndhhe1.ma.attbb.net [24.128.0.101]
 5  15 ms  15 ms  15 ms  12.125.47.49
 6  17 ms  17 ms  17 ms  12.123.40.218
 7  22 ms  23 ms  22 ms  tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
 8  23 ms  23 ms  23 ms  ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
 9  26 ms  21 ms  25 ms  att-gw.nyc.opentransit.net [192.205.32.138]
10  98 ms  98 ms  96 ms  P4-0.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
11  97 ms  98 ms  98 ms  P9-0.AUUCR1.Aubervilliers.opentransit.net [193.251.243.29]
12  98 ms  98 ms  108 ms  P6-0.BAGCR1.Bagnolet.opentransit.net [193.251.241.93]
13  104 ms  106 ms  103 ms  193.51.185.30
14  114 ms  114 ms  117 ms  grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
15  114 ms  115 ms  114 ms  nice-pos2-0.cssi.renater.fr [193.51.180.34]
16  129 ms  114 ms  118 ms  inria-nice.cssi.renater.fr [193.51.181.137]
17  113 ms  114 ms  112 ms  www.inria.fr [138.96.146.2]

Trace complete.
C:\WINDOWS\SYSTEM32>
```