

Question 2: Understanding ICMP

#2-A:

icmp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	0.001656	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x00000000
4	0.415098	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) request id=0x00000000

> Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da: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)

As seen in the above screenshot, the ICMP type is 8 and the code number is 0. The other fields that the ICMP packet has are: checksum, identifier, sequence number, and data. The checksum, sequence number and identifier fields all have 2 bytes of data each.

#2-B: Q8

icmp-ethereal-trace-2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x00000000
2	0.013151	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (TTL=1)
3	0.013258	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x00000000
4	0.025551	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (TTL=1)
5	0.025634	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x00000000
6	0.030171	10.216.228.1	192.168.1.101	ICMP	70	Time-to-live exceeded (TTL=1)
7	1.033537	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x00000000
8	1.054542	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (TTL=1)
9	1.054646	192.168.1.101	138.96.146.2	ICMP	106	Echo (ping) request id=0x00000000
10	1.068646	24.218.0.153	192.168.1.101	ICMP	70	Time-to-live exceeded (TTL=1)

> 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

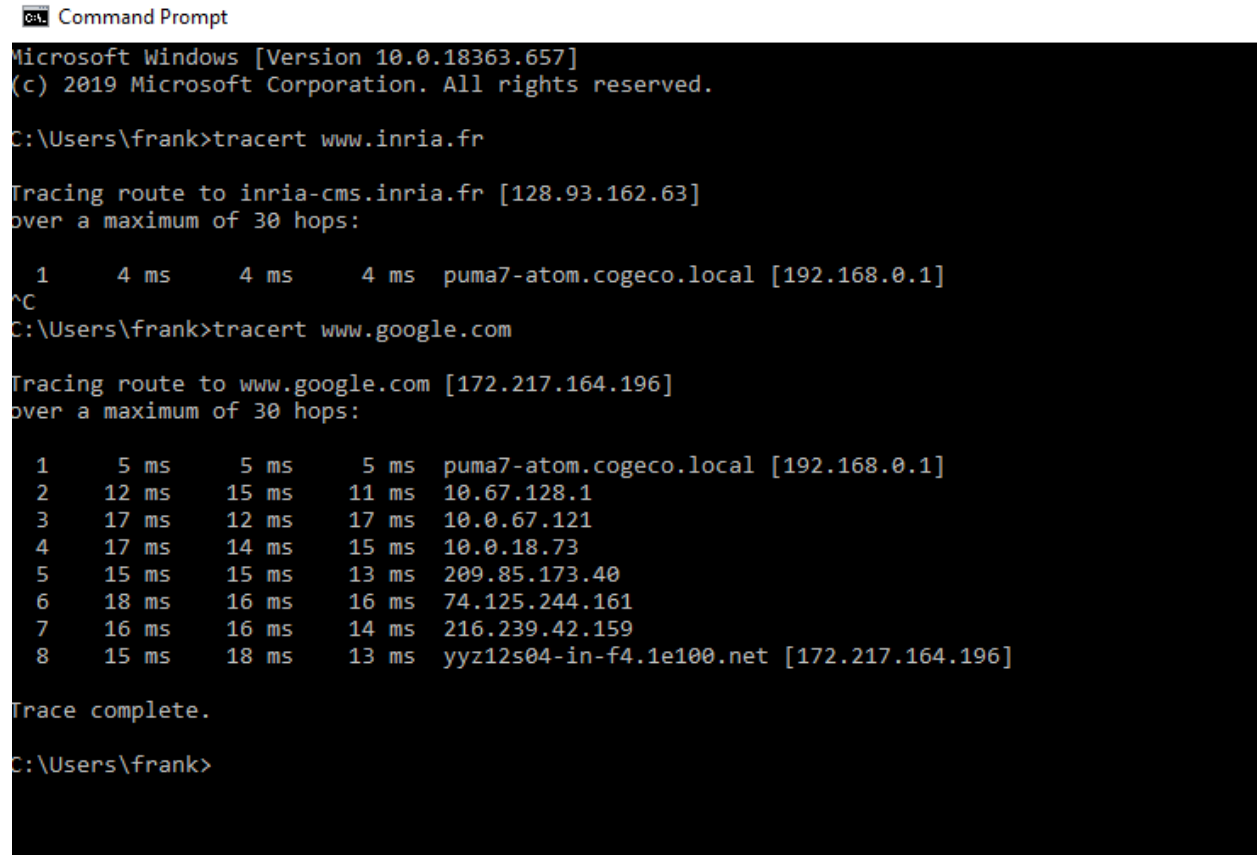
- Type: 8 (Echo (ping) request)
- Code: 0
- Checksum: 0x51fe [unverified] [in ICMP error packet] [Checksum Status: Unverified]
- Identifier (BE): 512 (0x0200)
- Identifier (LE): 2 (0x0002)
- Sequence number (BE): 41985 (0xa401)
- Sequence number (LE): 420 (0x01a4)

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 c0 ..tOgH...%..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..V..
 0030 00 00 01 01 d1 45 c0 a8 01 65 8a 60 92 02 08 00E....e.....
 0040 51 fe 02 00 a4 01 Q.....

Each time when the frame was captured (frame time, epoch) | Packets: 102 / Displayed: 102 (100.0%) | Profile: Default

As seen in the above screenshot, the ICMP error packet has both the IP header and the first 8 bytes of the original ICMP packet that the error is for.

#2-C:



```

C:\> Command Prompt
Microsoft Windows [Version 10.0.18363.657]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\frank>tracert www.inria.fr

Tracing route to inria-cms.inria.fr [128.93.162.63]
over a maximum of 30 hops:

  1      4 ms      4 ms      4 ms  puma7-atom.cogeco.local [192.168.0.1]
^C
C:\Users\frank>tracert www.google.com

Tracing route to www.google.com [172.217.164.196]
over a maximum of 30 hops:

  1      5 ms      5 ms      5 ms  puma7-atom.cogeco.local [192.168.0.1]
  2     12 ms     15 ms     11 ms  10.67.128.1
  3     17 ms     12 ms     17 ms  10.0.67.121
  4     17 ms     14 ms     15 ms  10.0.18.73
  5     15 ms     15 ms     13 ms  209.85.173.40
  6     18 ms     16 ms     16 ms  74.125.244.161
  7     16 ms     16 ms     14 ms  216.239.42.159
  8     15 ms     18 ms     13 ms  yyz12s04-in-f4.1e100.net [172.217.164.196]

Trace complete.

C:\Users\frank>

```

As shown in the screenshot, the tracert experiment to google.com produces results such that there are no significant delays between hops. In the total of 8 hops, all of them are within a couple of ms of each other, which is drastically different from Q10 in the ICMP lab, where there was a delay of over 100 ms.