Lab 05_ICMP

Part 1: ICMP AND PING

```
Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=56ms TTL=51
Reply from 143.89.12.134: bytes=32 time=88ms TTL=51
Reply from 143.89.12.134: bytes=32 time=58ms TTL=51
Reply from 143.89.12.134: bytes=32 time=53ms TTL=51
Reply from 143.89.12.134: bytes=32 time=55ms TTL=51
Reply from 143.89.12.134: bytes=32 time=55ms TTL=51
Reply from 143.89.12.134: bytes=32 time=56ms TTL=51
Reply from 143.89.12.134: bytes=32 time=54ms TTL=51
Reply from 143.89.12.134: bytes=32 time=54ms TTL=51
Reply from 143.89.12.134: bytes=32 time=53ms TTL=51

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 53ms, Maximum = 88ms, Average = 58ms

C:\Users\DELL>
```

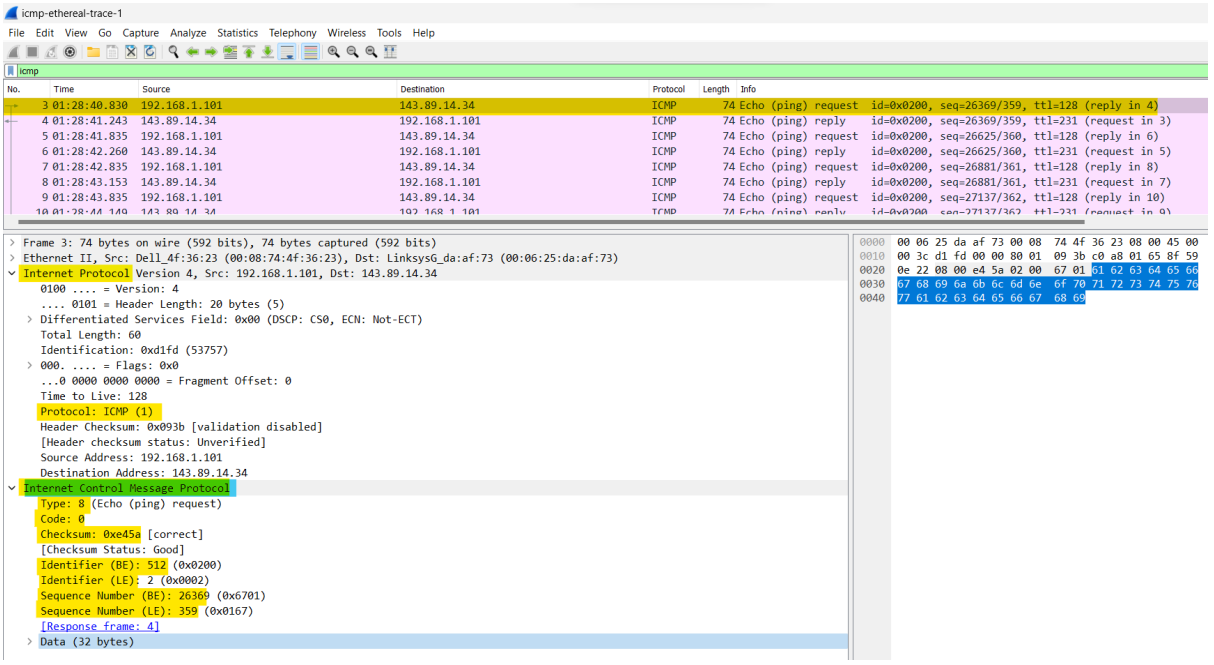
1. **. What is the IP address of your host? What is the IP address of the destination host?**

   The IP address of my host: 192.168.1.101

   The IP address of the destination host: 143.89.14.134

2. **Why is it that an ICMP packet does not have source and destination port numbers?**

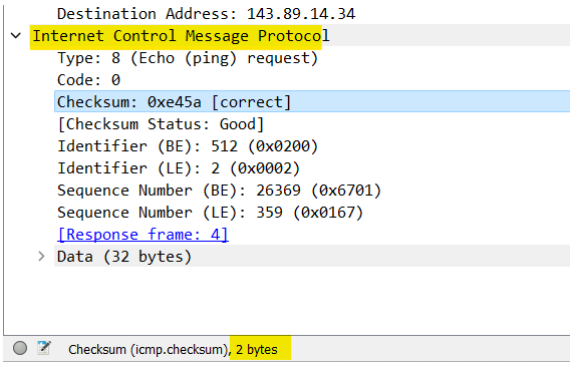
   The ICMP packet does not have source and destination port numbers because it was designed to communicate network-layer information between hosts and routers, not between application layer processes. Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

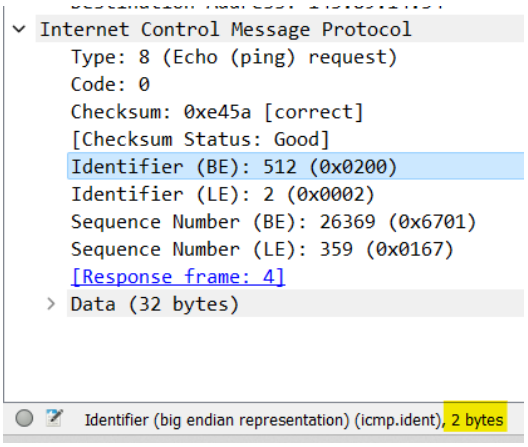


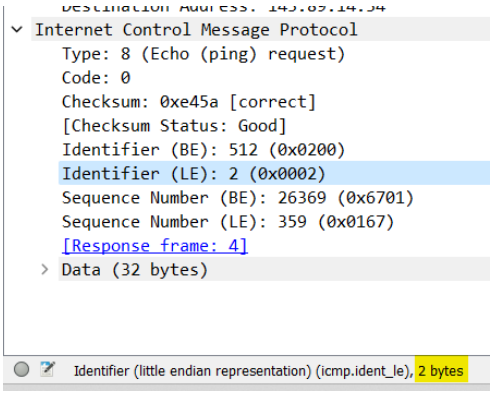
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?

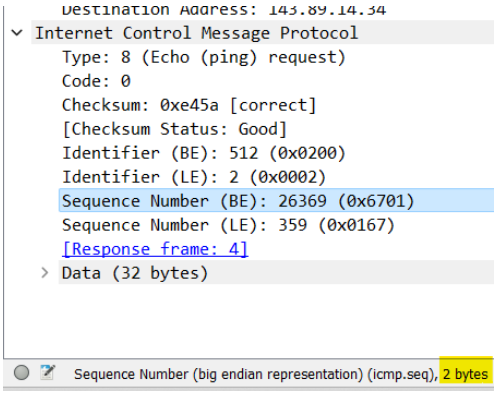
The ICMP type is 8, and the code number is 0.

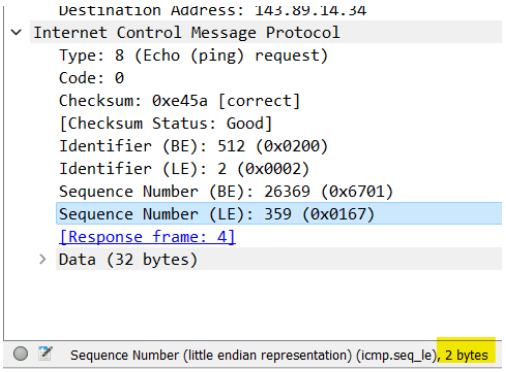
The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.







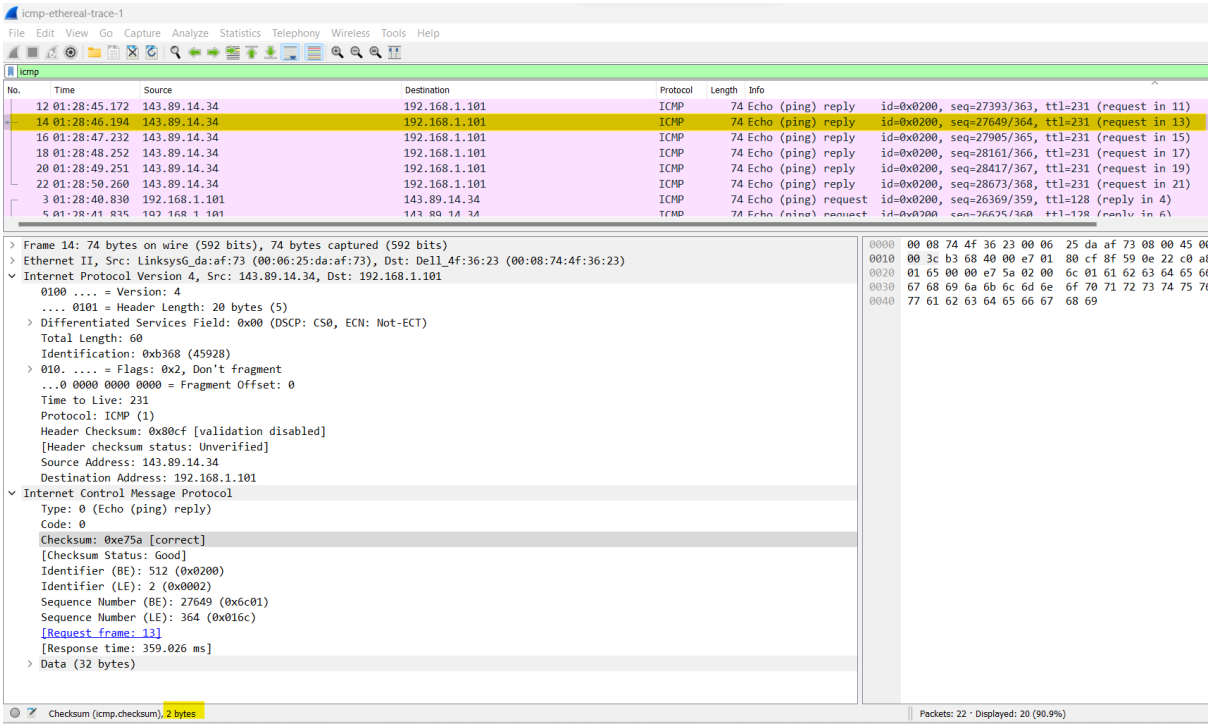




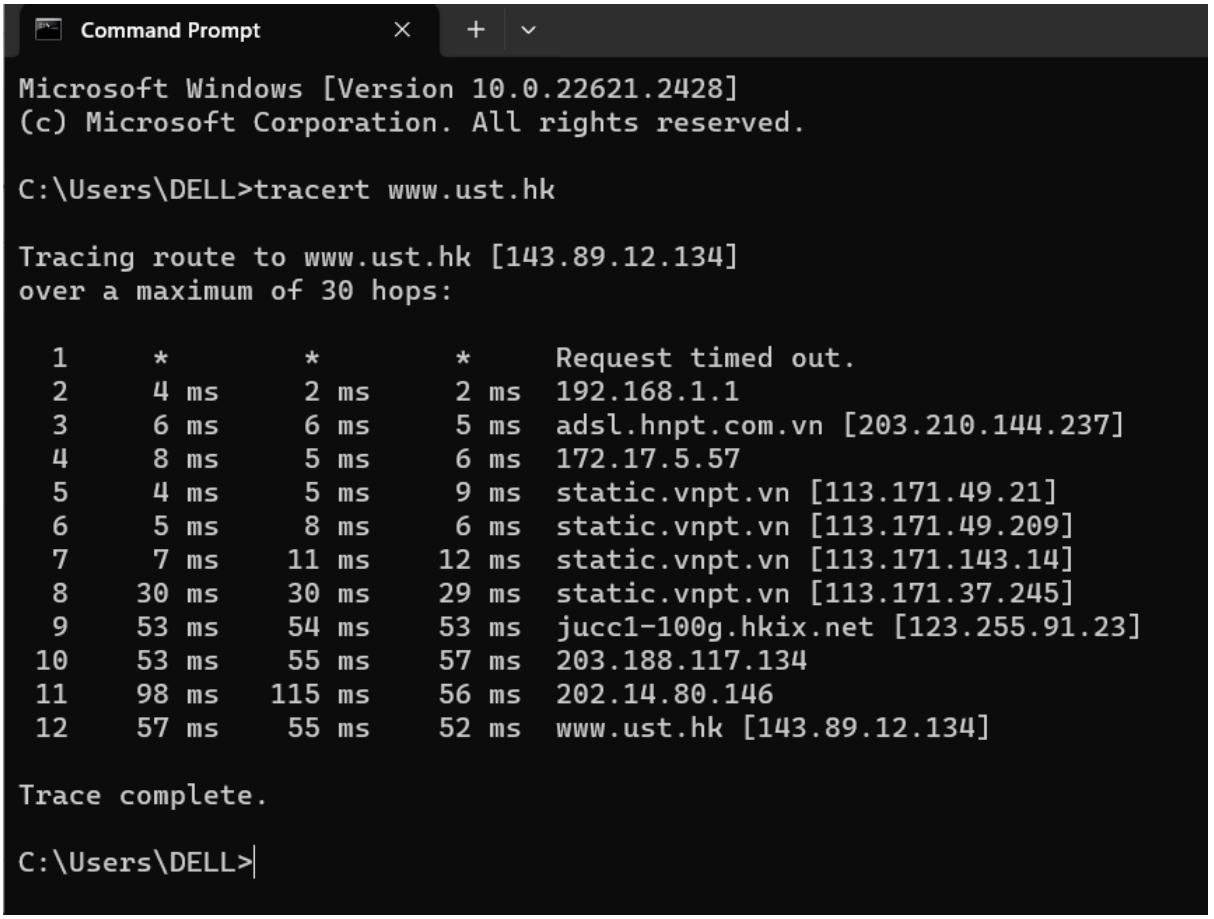
4. **Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?**

   The ICMP type is 8, and the code number is 0.

   The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.



PART 2. ICMP and Traceroute



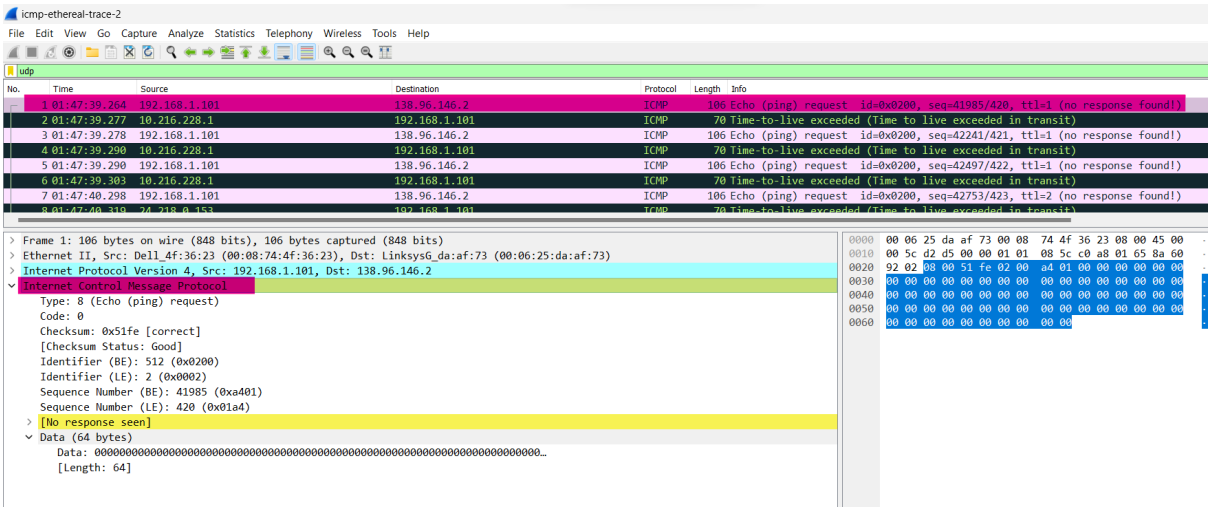
```
Command Prompt

Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>tracert www.ust.hk

Tracing route to www.ust.hk [143.89.12.134]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     4 ms     2 ms     2 ms  192.168.1.1
  3     6 ms     6 ms     5 ms  adsl.hnpt.com.vn [203.210.144.237]
  4     8 ms     5 ms     6 ms  172.17.5.57
  5     4 ms     5 ms     9 ms  static.vnpt.vn [113.171.49.21]
  6     5 ms     8 ms     6 ms  static.vnpt.vn [113.171.49.209]
  7     7 ms    11 ms    12 ms  static.vnpt.vn [113.171.143.14]
  8    30 ms    30 ms    29 ms  static.vnpt.vn [113.171.37.245]
  9    53 ms    54 ms    53 ms  jucc1-100g.hkix.net [123.255.91.23]
 10    53 ms    55 ms    57 ms  203.188.117.134
 11    98 ms   115 ms    56 ms  202.14.80.146
 12    57 ms    55 ms    52 ms  www.ust.hk [143.89.12.134]

Trace complete.

C:\Users\DELL>
```

5. **What is the IP address of your host? What is the IP address of the target destination host?**

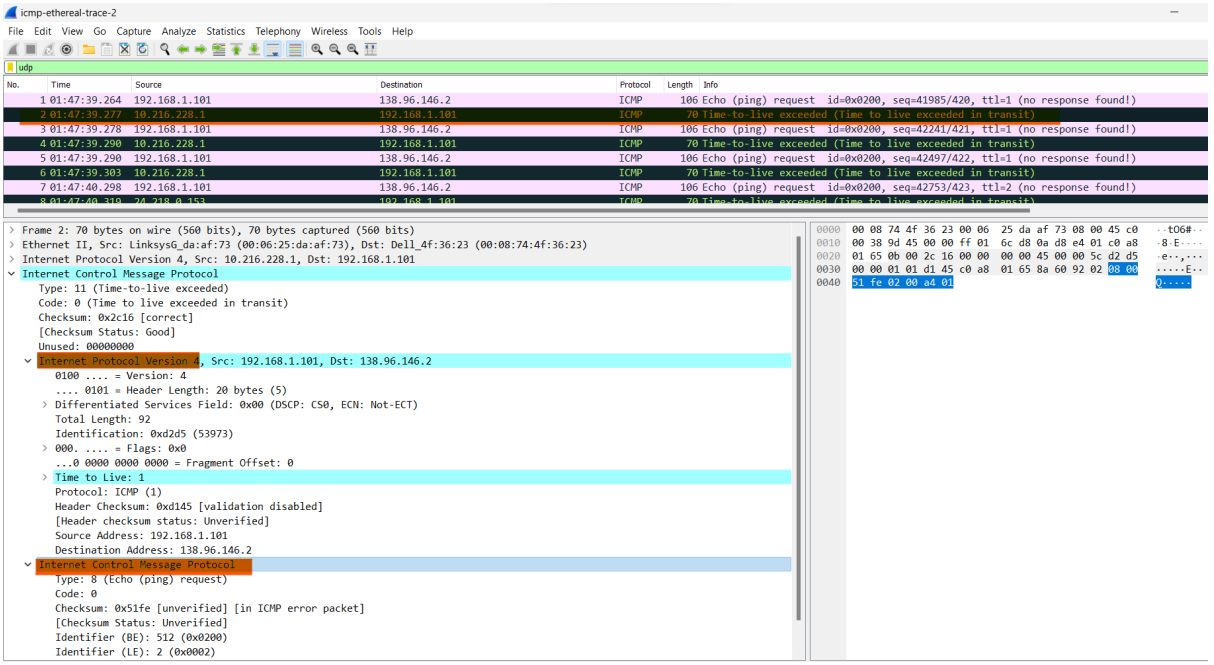
The IP address of my host: 192.168.1.101
The IP address of the destination host: 138.96.146.2

6. **If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?**
   No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

7. **Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?**
   The ICMP echo packet has the same fields as the ping query packets.

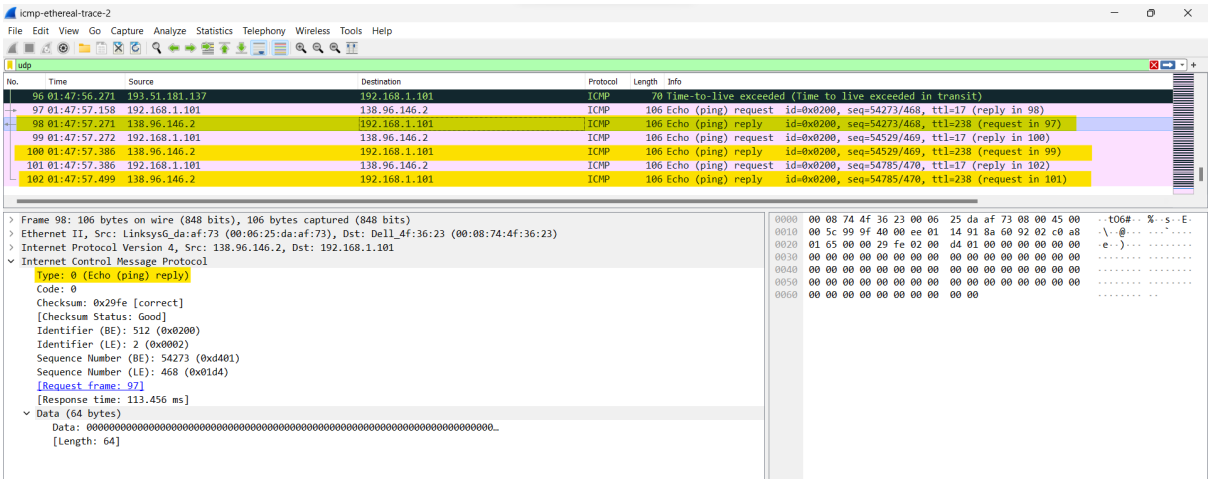


8. **Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?**
   The ICMP error packet is not the same as the ICMP echo packet. It contains both the IP header (ipv4 fields) and the first 8 bytes of the original ICMP packet that the error is for.



9. **Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?**

   The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired). They are different because the datagrams have made it all the way to the destination host before the TTL expired.



10. **Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?**

In figure 4: there is a link whose delay is significantly longer than the others at 9 to 10.

Within the tracert measurements, there is a link whose delay is significantly longer than the others at 8 to 10.

It looks like it is somewhere in France.

```
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.wsfdhe1.ma.attbb.net [24.128.190.197]
  4    16 ms    16 ms    15 ms  bar02-p6-0.ndhmhe1.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.AUVCR1.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>_
```

Figure 4 Command Prompt window displays the results of the Traceroute program.

```
Command Prompt
Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

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

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

  1     *        *        *     Request timed out.
  2     3 ms     2 ms     2 ms  192.168.1.1
  3     4 ms     7 ms     5 ms  adsl.hnpt.com.vn [203.210.144.237]
  4     5 ms     8 ms     8 ms  172.17.5.61
  5     7 ms     5 ms     5 ms  static.vnpt.vn [113.171.48.57]
  6    41 ms    39 ms    41 ms  static.vnpt.vn [113.171.7.33]
  7    46 ms    46 ms    45 ms  static.vnpt.vn [113.171.50.222]
  8    40 ms    41 ms    40 ms  static.vnpt.vn [113.171.36.53]
  9     *        *        *     Request timed out.
 10   211 ms   211 ms   213 ms  et-5-0-1-ren-nr-paris1-rtr-131.noc.renater.fr [193.55.204.194]
 11   211 ms   211 ms   211 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 12   212 ms   213 ms   212 ms  inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 13   211 ms   211 ms   210 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 14   213 ms   211 ms   211 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\DELL>
```

my Figure: Command prompt for traceroute