

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.

icmpe-ethereal-trace-1

No.	Time	Source	Destination	Protocol	Length	Info
3	01:28:40.830	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
4	01:28:41.243	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26369/359, ttl=128 (request in 3)
5	01:28:41.835	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)
6	01:28:42.260	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26625/360, ttl=128 (request in 5)
7	01:28:42.835	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26881/361, ttl=128 (reply in 8)
8	01:28:43.153	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=26881/361, ttl=128 (request in 7)
9	01:28:43.835	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=27137/362, ttl=128 (reply in 10)
10	01:28:44.140	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27137/362, ttl=128 (request in 9)

> 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: Linksys_0a:af:73 (00:06:25:da:af:73)

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

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0xd1fd (53757)

> 0000 = Flags: 0x00

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

Header Checksum: 0x093b [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.1.101

Destination Address: 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)

- 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.

Destination Address: 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)

Checksum (icmp.checksum), 2 bytes

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)

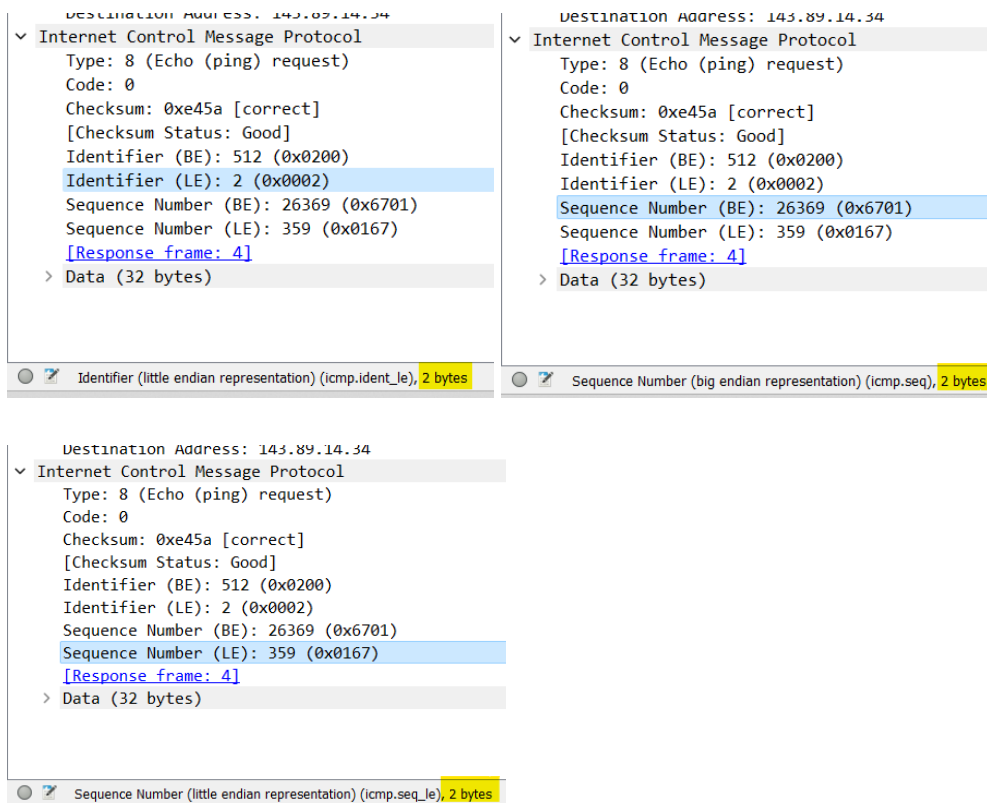
Sequence Number (BE): 26369 (0x6701)

Sequence Number (LE): 359 (0x0167)

[Response frame: 4]

> Data (32 bytes)

Identifier (big endian representation) (icmp.ident), 2 bytes



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.

icmp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
12	01:28:45.172	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27393/363, ttl=231 (request in 11)
14	01:28:46.194	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27649/364, ttl=231 (request in 13)
16	01:28:47.232	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=27905/365, ttl=231 (request in 15)
18	01:28:48.252	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=28161/366, ttl=231 (request in 17)
20	01:28:49.251	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=28417/367, ttl=231 (request in 19)
22	01:28:50.260	143.89.14.34	192.168.1.101	ICMP	74	Echo (ping) reply id=0x0200, seq=28673/368, ttl=231 (request in 21)
3	01:28:40.830	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26369/359, ttl=128 (reply in 4)
5	01:28:41.835	192.168.1.101	143.89.14.34	ICMP	74	Echo (ping) request id=0x0200, seq=26625/360, ttl=128 (reply in 6)

> Frame 14: 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

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0xb368 (45928)

> 010 = Flags: 0x2, Don't fragment

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 231

Protocol: ICMP (1)

Header Checksum: 0x80cf [validation disabled]

[Header checksum status: Unverified]

Source Address: 143.89.14.34

Destination Address: 192.168.1.101

> Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xe75a [correct]

[Checksum Status: Good]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 27649 (0x6c01)

Sequence Number (LE): 364 (0x016c)

[Request frame: 13]

[Response time: 359.026 ms]

> Data (32 bytes)

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 04
0010 00 3c b3 68 40 00 e7 01 80 cf 8f 59 0e 22 c0 af
0020 01 65 00 00 e7 5a 02 00 6c 01 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69

Checksum (icmp.checksum), 2 bytes

Packets: 22 · Displayed: 20 (90.9%)

PART 2. ICMP and Traceroute

```

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>

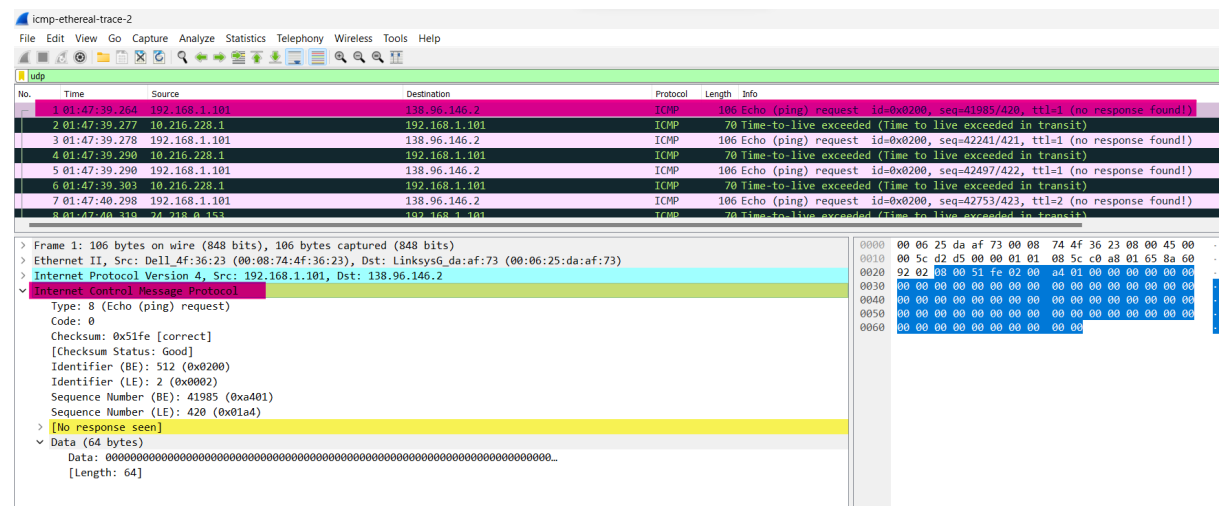
```

- What is the IP address of your host? What is the IP address of the target destination host?

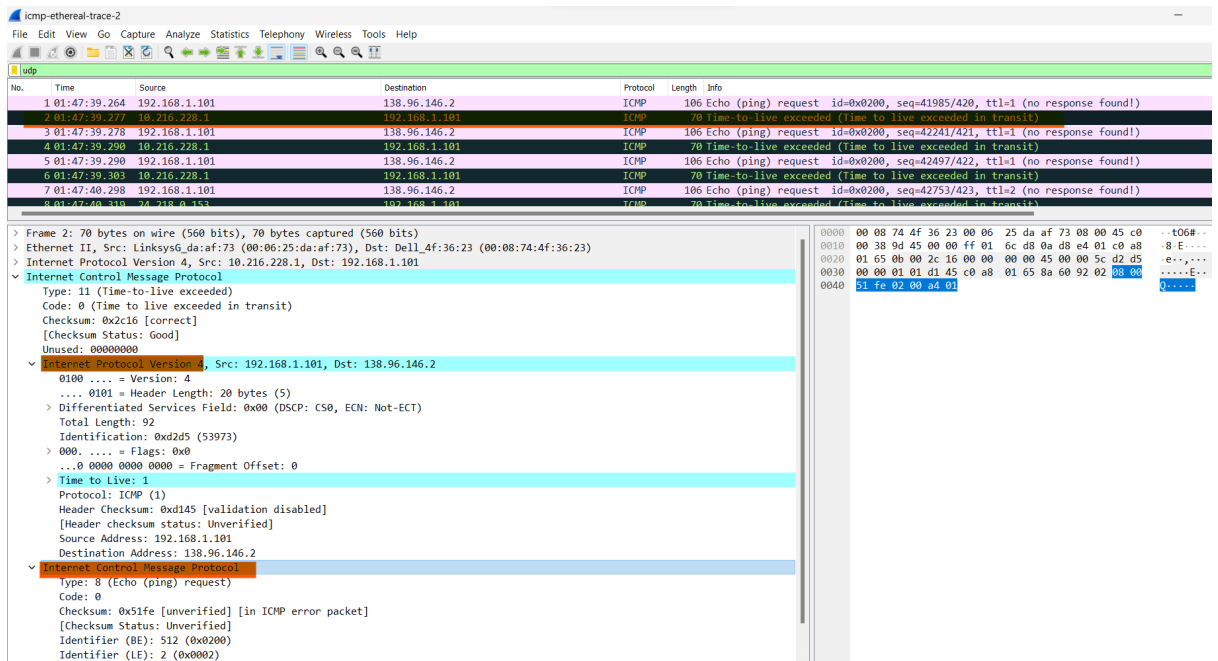
The IP address of the destination host: 138.96.146.2

No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11

The ICMP echo packet has the same fields as the ping query packets.

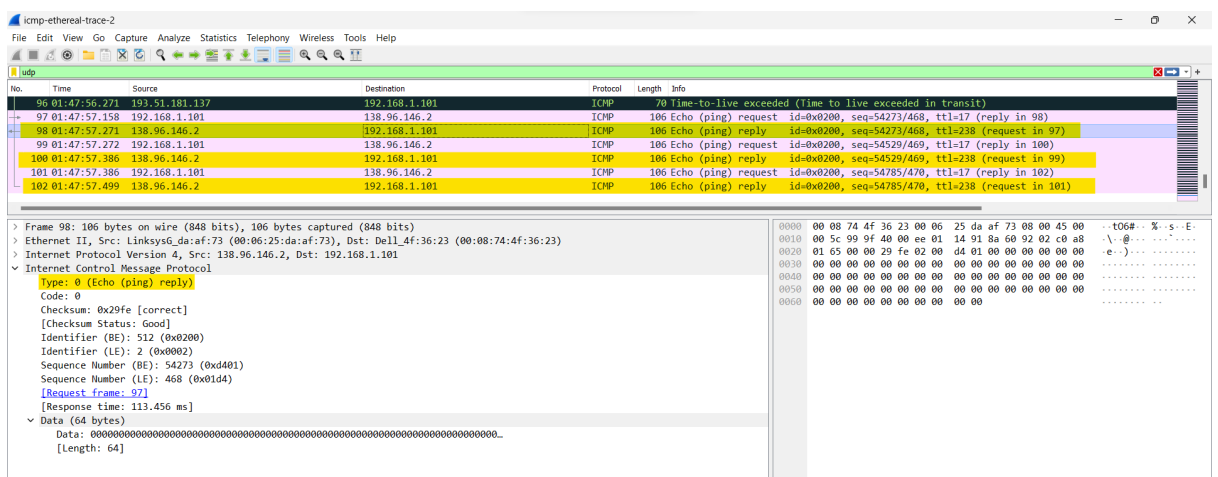


The ICMP error packet is not the same as the ICMP echo packet. It contains both the IP header (ipv4 fields) and the first 8 bytes of the original ICMP packet that the error is for.



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.

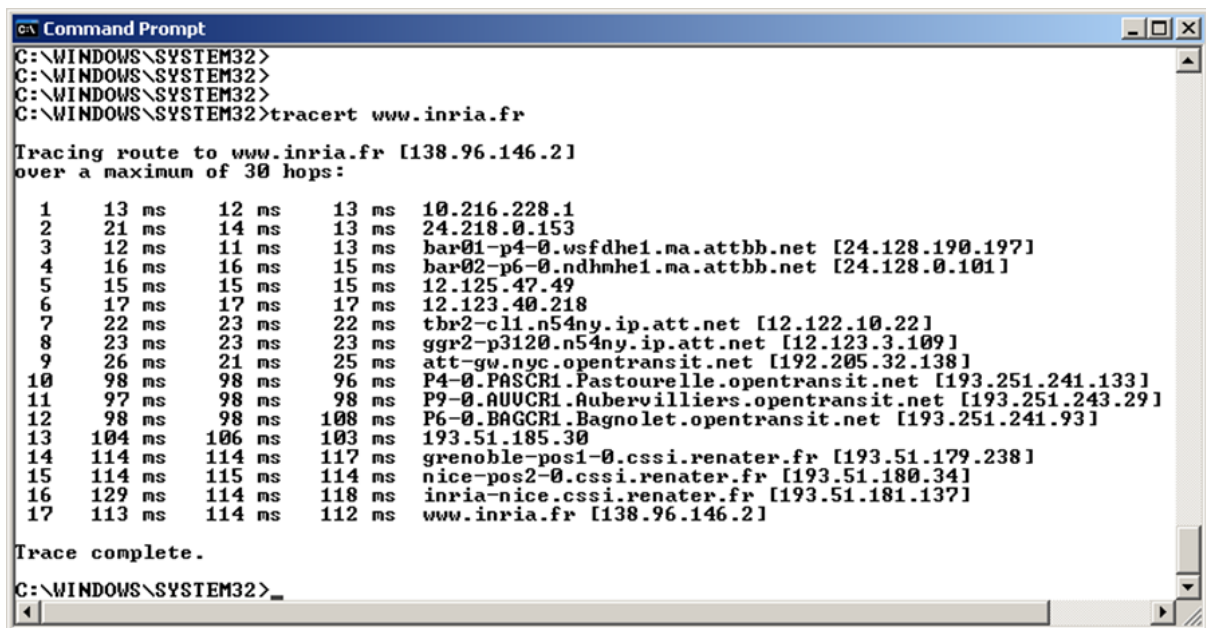


10. Within the traceroute measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of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

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

Within the traceroute 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.

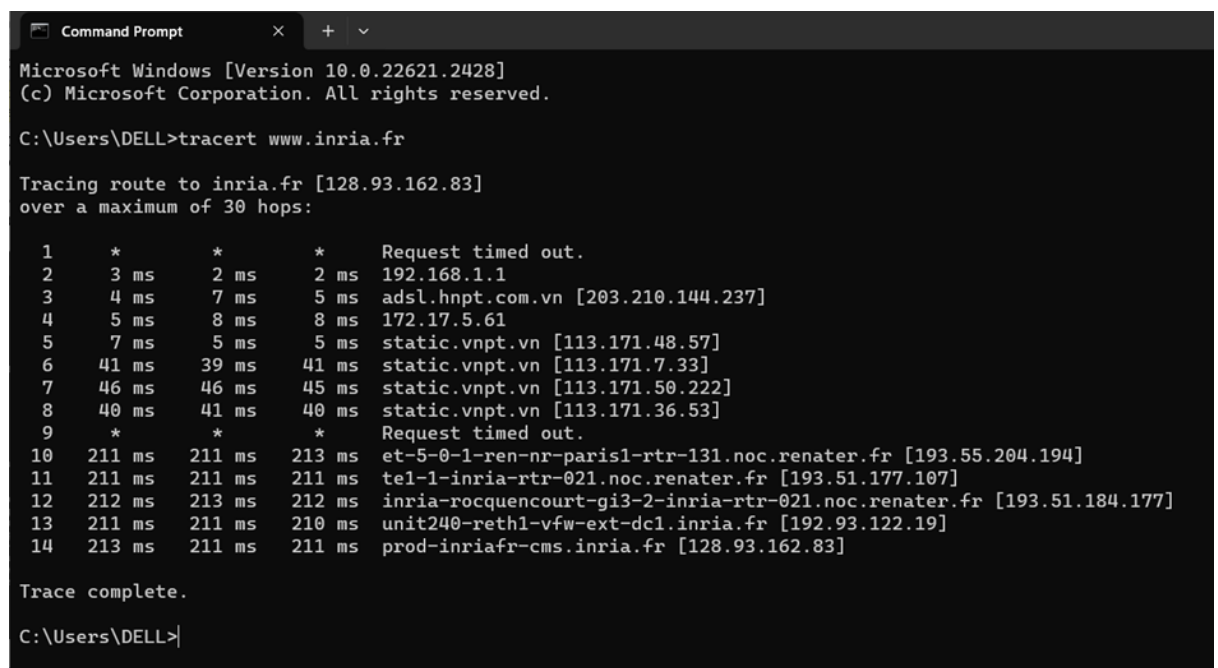


```
Command Prompt
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>
C:\WINDOWS\SYSTEM32>tracert www.inria.fr

Tracing route to www.inria.fr [138.96.146.2]
over a maximum of 30 hops:
  0  13 ms  12 ms  13 ms  10.216.228.1
  1  21 ms  14 ms  13 ms  24.218.0.153
  2  12 ms  11 ms  13 ms  bar01-p4-0.wsfde1.ma.attbb.net [24.128.190.197]
  3  16 ms  16 ms  15 ms  bar02-p6-0.ndhmhe1.ma.attbb.net [24.128.0.101]
  4  15 ms  15 ms  15 ms  12.125.47.49
  5  17 ms  17 ms  17 ms  12.123.40.218
  6  22 ms  23 ms  22 ms  tbr2-cl1.n54ny.ip.att.net [12.122.10.22]
  7  23 ms  23 ms  23 ms  ggr2-p3120.n54ny.ip.att.net [12.123.3.109]
  8  26 ms  21 ms  25 ms  att-gw.nyc.opentransit.net [192.205.32.138]
  9  98 ms  98 ms  96 ms  P4-0.PASCRI.Pastourelle.opentransit.net [193.251.241.133]
 10  97 ms  98 ms  98 ms  P9-0.AUUCRI.Aubervilliers.opentransit.net [193.251.243.29]
 11  98 ms  98 ms  108 ms  P6-0.BAGCRI.Bagnolet.opentransit.net [193.251.241.93]
 12 104 ms 106 ms 103 ms 193.51.185.30
 13 114 ms 114 ms 117 ms grenoble-pos1-0.cssi.renater.fr [193.51.179.238]
 14 114 ms 115 ms 114 ms nice-pos2-0.cssi.renater.fr [193.51.180.34]
 15 129 ms 114 ms 118 ms inria-nice.cssi.renater.fr [193.51.181.137]
 16 113 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:
  0  *      *      *      Request timed out.
  1  3 ms   2 ms   2 ms   192.168.1.1
  2  4 ms   7 ms   5 ms   adsl.hnpt.com.vn [203.210.144.237]
  3  5 ms   8 ms   8 ms   172.17.5.61
  4  7 ms   5 ms   5 ms   static.vnpt.vn [113.171.48.57]
  5  41 ms  39 ms  41 ms   static.vnpt.vn [113.171.7.33]
  6  46 ms  46 ms  45 ms   static.vnpt.vn [113.171.50.222]
  7  40 ms  41 ms  40 ms   static.vnpt.vn [113.171.36.53]
  8  *      *      *      Request timed out.
  9  211 ms 211 ms 213 ms et-5-0-1-ren-nr-paris1-rtr-131.noc.renater.fr [193.55.204.194]
 10 211 ms 211 ms 211 ms tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 11 212 ms 213 ms 212 ms inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 12 211 ms 211 ms 210 ms unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 13 213 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