

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH  
TRƯỜNG ĐẠI HỌC BÁCH KHOA  
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH



**MẠNG MÁY TÍNH (CO3094)**

---

**Báo cáo Lab 2\_5: Wireshark Lab – ICMP**

---

Giảng viên: Nguyễn Tấn Đạt  
SV thực hiện: Đinh Như Tân – 1915040

Tp. Hồ Chí Minh, Tháng 10/2021

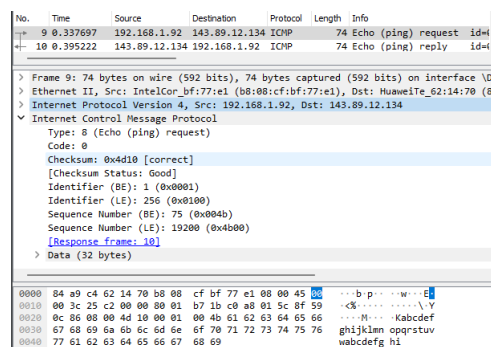
```
C:\Windows\System32>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=57ms TTL=46
Reply from 143.89.12.134: bytes=32 time=57ms TTL=46
Reply from 143.89.12.134: bytes=32 time=56ms TTL=46
Reply from 143.89.12.134: bytes=32 time=56ms TTL=46
Reply from 143.89.12.134: bytes=32 time=55ms TTL=46
Reply from 143.89.12.134: bytes=32 time=58ms TTL=46
Reply from 143.89.12.134: bytes=32 time=170ms TTL=46
Reply from 143.89.12.134: bytes=32 time=56ms TTL=46
Reply from 143.89.12.134: bytes=32 time=102ms TTL=46
Reply from 143.89.12.134: bytes=32 time=56ms TTL=46

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 170ms, Average = 72ms
```

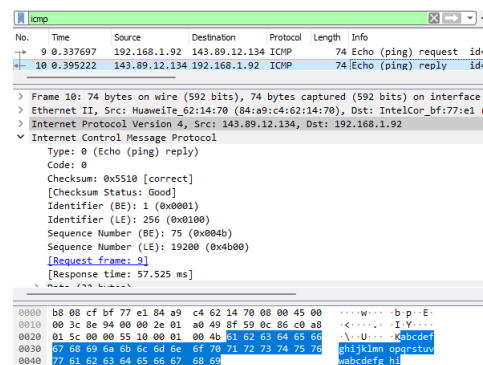
Hình 1: Command prompt after ping request

- What is the IP address of your host? What is the IP address of the destination host?  
*The IP address of my host is 192.168.1.92. The IP address of the destination host is 143.89.12.134*
- 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.*



Hình 2: ICMP Echo Request message

- 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.*

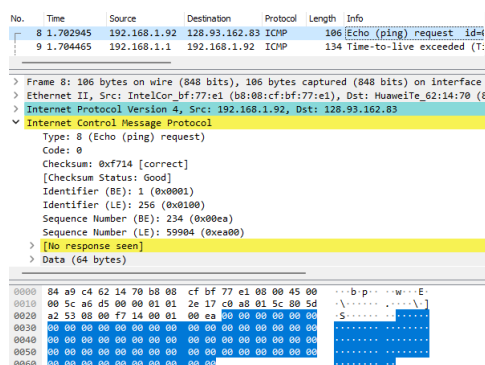


Hình 3: ICMP Echo Reply message

- 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?

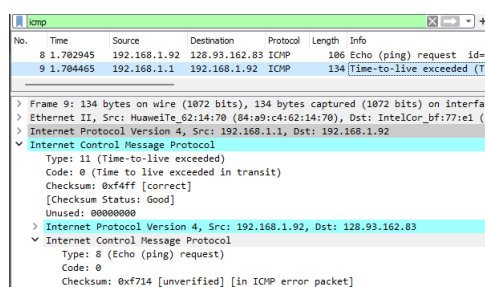
The ICMP type is 0, and the code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

- What is the IP address of your host? What is the IP address of the target destination host?  
*The IP address of my host is 192.168.1.92. The IP address of the destination host is 128.93.162.83*
- 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*



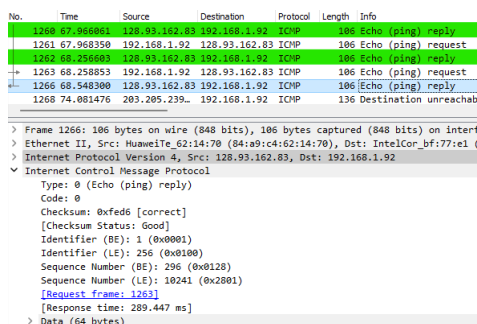
Hình 4: ICMP echo request packet

- 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.*



Hình 5: ICMP echo error packet

- 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 ping query packets. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.*



Hình 6: Last three ICMP reply packets

- 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.

```
C:\Windows\System32>tracert www.inria.fr
Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:
  0  1 ms  1 ms  1 ms  192.168.1.1
  1  7 ms  17 ms  24 ms  100.117.0.2
  2  6 ms  5 ms  5 ms  172.16.29.45
  3  10 ms  10 ms  10 ms  172.16.66.1
  4  *  *  *  Request timed out.
  5  11 ms  *  12 ms  172.16.67.109
  6  13 ms  12 ms  13 ms  10.255.10.15
  7  52 ms  54 ms  53 ms  NHUTAN_CS [27.68.229.13]
  8  50 ms  45 ms  45 ms  NHUTAN_CS [27.68.255.38]
  9  45 ms  45 ms  46 ms  NHUTAN_CS [27.68.250.32]
 10  45 ms  46 ms  44 ms  NHUTAN_CS [27.68.240.196]
 11  51 ms  51 ms  52 ms  te0-0-0-23.c1br01.hkg04.pccwbtn.net [63.216.84.65]
 12  48 ms  46 ms  46 ms  HundredGE0-0-0-2.br02.hkg12.pccwbtn.net [63.218.174.85]
 13  46 ms  46 ms  46 ms  HundredGE0-0-0-2.br02.hkg12.pccwbtn.net [63.218.174.85]
 14  58 ms  60 ms  58 ms  ae5.cr0-hkg2.ip4.gtt.net [69.174.124.169]
 15  201 ms  202 ms  201 ms  et-3-3-0-cr2-par7.ip4.gtt.net [213.200.119.214]
 16  301 ms  292 ms  289 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 17  300 ms  290 ms  294 ms  te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 18  287 ms  289 ms  296 ms  inria-rocquencourt-g13-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
 19  293 ms  291 ms  295 ms  unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 20  298 ms  288 ms  289 ms  prod-inriafr-cms.inria.fr [128.93.162.83]
Trace complete.
```

Hình 7: Command prompt for traceroute

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?

There is a link between steps 11 and 12 that has a significantly longer delay. This is a transatlantic link from New York to Aubervilliers, France. In figure 4 from the lab, the link is from New York to Pastourelle, France.