

TRƯỜNG ĐẠI HỌC BÁCH KHOA
ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH



HOMEWORK
MẠNG MÁY TÍNH (THỰC HÀNH) – LAB 5

Giảng viên hướng dẫn: Ths. Bùi Xuân Giang

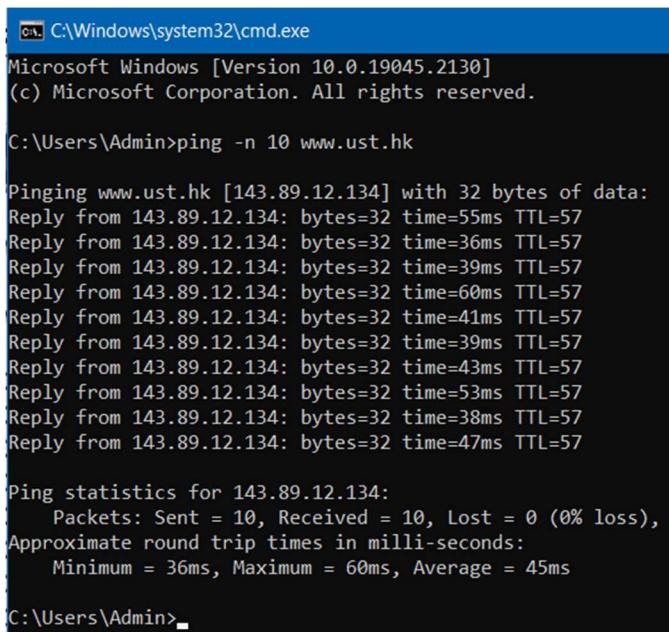
Sinh viên thực hiện: Trần Minh Tân

Mã số sinh viên: 2012018

Lớp: L10.

PART I. ICMP and Ping.

This is the picture of my CMD



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2130]
(c) Microsoft Corporation. All rights reserved.

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

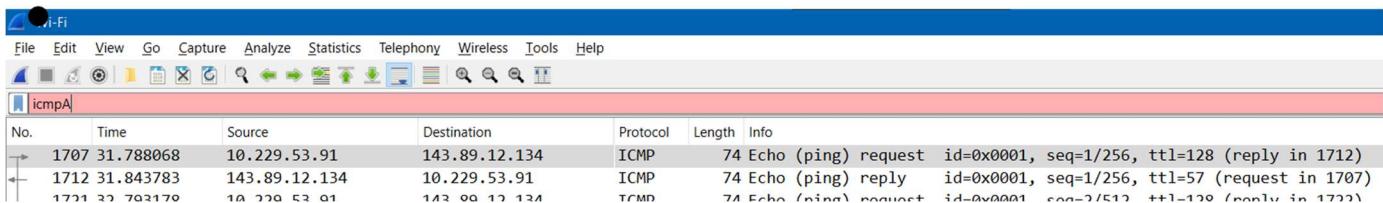
Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=55ms TTL=57
Reply from 143.89.12.134: bytes=32 time=36ms TTL=57
Reply from 143.89.12.134: bytes=32 time=39ms TTL=57
Reply from 143.89.12.134: bytes=32 time=60ms TTL=57
Reply from 143.89.12.134: bytes=32 time=41ms TTL=57
Reply from 143.89.12.134: bytes=32 time=39ms TTL=57
Reply from 143.89.12.134: bytes=32 time=43ms TTL=57
Reply from 143.89.12.134: bytes=32 time=53ms TTL=57
Reply from 143.89.12.134: bytes=32 time=38ms TTL=57
Reply from 143.89.12.134: bytes=32 time=47ms TTL=57

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 60ms, Average = 45ms

C:\Users\Admin>
```

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

The IP address of my host is 10.229.53.91. The destination host is 143.89.12.134



No.	Time	Source	Destination	Protocol	Length	Info
1707	31.788068	10.229.53.91	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1707)
1712	31.843783	143.89.12.134	10.229.53.91	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=57 (request in 1707)
1721	32.702170	10.229.53.91	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001 seq=2/256 ttl=128 (reply in 1722)

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

TCP and UDP are transport protocols that use port numbers to multiplex their use between applications or processes. ICMP is not a transport protocol but a part of the IP protocol. It is used for signaling between hosts.

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 ?

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpA

No.	Time	Source	Destination	Protocol	Length	Info
1707	31.788068	10.229.53.91	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1712)

```

> Frame 1707: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F773D61D
> Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)
> Internet Protocol Version 4, Src: 10.229.53.91, Dst: 143.89.12.134
└ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d5a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 1712]
    Data (32 bytes)
        Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
        [Length: 32]

```

The ICMP type and code is 8 and 0 respectively.

The other fields are Checksum , Identifier and Sequence Number.

The checksum , sequence number and identifier fields are all 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?

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmpA

No.	Time	Source	Destination	Protocol	Length	Info
1707	31.788068	10.229.53.91	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 1712)
1712	31.843783	143.89.12.134	10.229.53.91	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=57 (request in 1707)
1721	32.793178	10.229.53.91	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 1722)

```

> Frame 1712: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{F773D61D
> Ethernet II, Src: HewlettP_a6:09:74 (f4:ce:46:a6:09:74), Dst: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)
> Internet Protocol Version 4, Src: 143.89.12.134, Dst: 10.229.53.91
└ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x555a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 1707]
    [Response time: 55.715 ms]

```

The ICMP type and code is 0 and 0 respectively.

The other fields are Checksum , Identifier and Sequence Number.

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

PART 2. ICMP and Traceroute

```

C:\Windows\system32\cmd.exe
15 327 ms 333 ms 324 ms unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
16 335 ms 344 ms 358 ms prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

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

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

 1  75 ms      3 ms      9 ms  10.229.0.1
 2  1750 ms    350 ms    180 ms static.cmcti.vn [203.205.56.22]
 3  15 ms      8 ms     19 ms static.cmcti.vn [203.205.56.124]
 4  773 ms      *      354 ms static.cmcti.vn [101.99.48.18]
 5  213 ms     176 ms     50 ms  203.131.243.65
 6  91 ms      69 ms     43 ms ae-11.r26.tkokhk01.hk.bb.gin.ntt.net [129.250.6.122]
 7  119 ms     122 ms     156 ms ae-12.r30.tokyjp05.jp.bb.gin.ntt.net [129.250.2.50]
 8  1670 ms      *     1832 ms ae-4.r25.snjsc04.us.bb.gin.ntt.net [129.250.5.78]
 9  648 ms     255 ms     298 ms ae-45.r01.snjsc04.us.bb.gin.ntt.net [129.250.3.175]
10  1956 ms      *     825 ms ae9.cr6-sjc1.ip4.gtt.net [69.174.23.157]
11  474 ms     290 ms     290 ms et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
12  362 ms     334 ms     634 ms renater-gw-ix1.gtt.net [77.67.123.206]
13  339 ms     327 ms     325 ms te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
14  328 ms     325 ms     351 ms inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
15      *     606 ms     362 ms unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
16  348 ms      *     470 ms prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

```

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 is 10.229.53.91

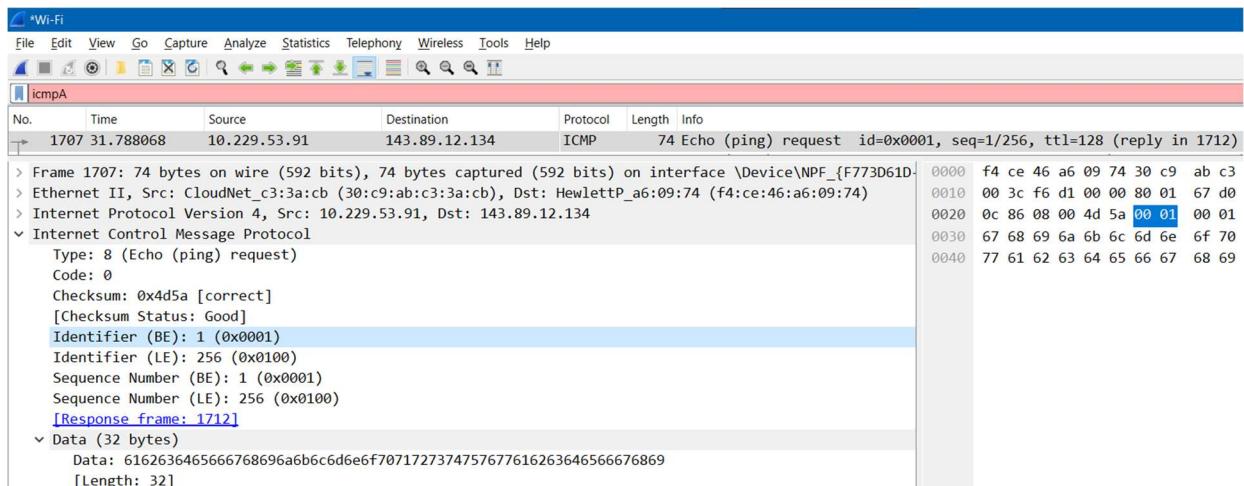
What is the IP address of the target destination host ? 128.93.162.83

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?

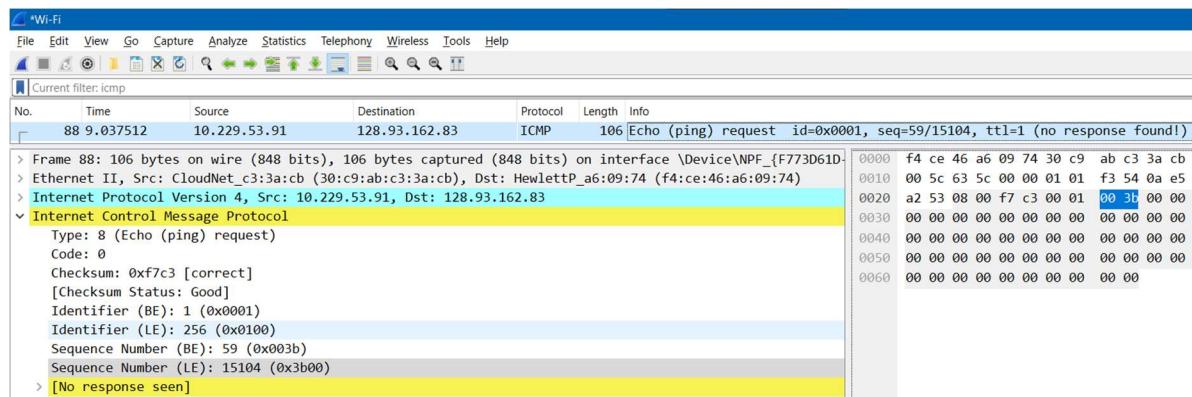
No, It would be 0x11.

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?

This is the ICMP ping query packet.



This is the ICMP echo packet in the second half of the lab



There are no differences between them. The fields are the same.

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?

This is the screenshot of the ICMP error packet.

The fields included the information of the error packet as well as IPv4 fields.

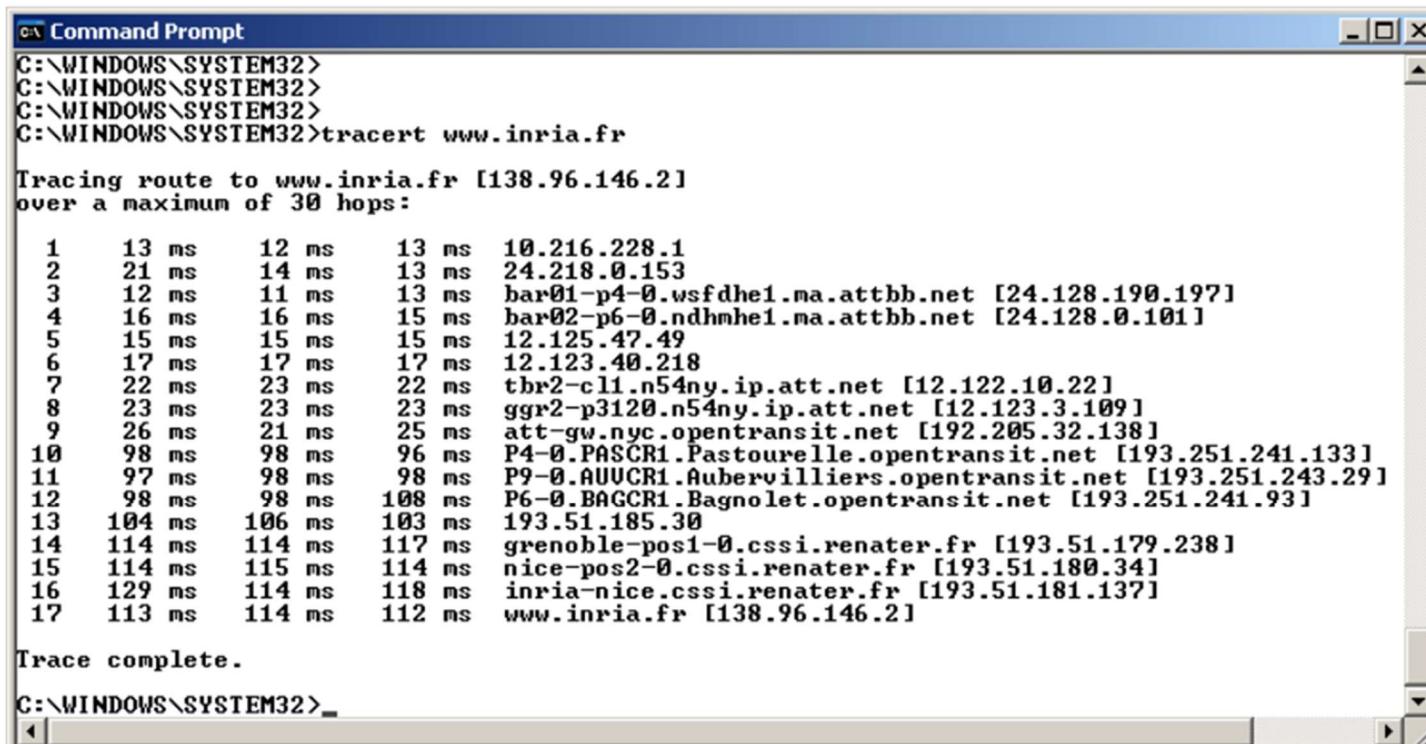
9. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?

They are different from the ICMP error packets because they have the response time field and they don't have the information of the error packet. Moreover, their type are 0, while the type of ICMP error packet is 8.

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?

Yes, the link at 9 to 10 are the one whose delay is significantly longer than others.

The location of the two routers on the end of this link is New York City, base on the "nyc" in line 9.



```
c:\ 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.wsfldhe1.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-c11.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>
```