

**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.

Thành phố Hồ Chí Minh – 2022

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

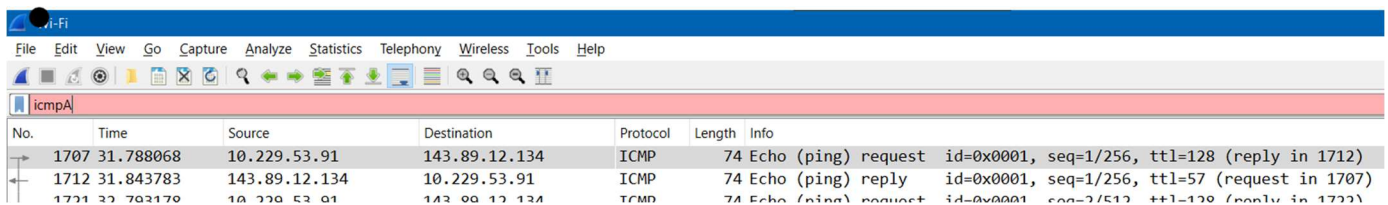
Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=55ms TTL=57
Reply from 143.89.12.134: bytes=32 time=36ms TTL=57
Reply from 143.89.12.134: bytes=32 time=39ms TTL=57
Reply from 143.89.12.134: bytes=32 time=60ms TTL=57
Reply from 143.89.12.134: bytes=32 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 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	32.702170	10.229.53.91	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, 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 ?

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-0000-f4 ce 46 a6 09 74 30 c9 ab c3}						
> 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?

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-0000-30 c9 ab c3 3a cb f4 ce 46 a6 09 74}						
> 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.snjsca04.us.bb.gin.ntt.net [129.250.5.78]
 9 648 ms 255 ms 298 ms ae-45.r01.snjsca04.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.

Wireshark packet capture showing an ICMP Echo (ping) request. The packet details are as follows:

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

Packet details:

- 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]

Packet bytes (hexadecimal):

```

0000 f4 ce 46 a6 09 74 30 c9 ab c3
0010 00 3c f6 d1 00 00 80 01 67 d0
0020 0c 86 08 00 4d 5a 00 01 00 01
0030 67 68 69 6a 6b 6c 6d 6e 6f 70
0040 77 61 62 63 64 65 66 67 68 69

```


Wireshark interface showing a packet capture on the 'Wi-Fi' interface. The packet list displays a single packet (No. 88) at time 88.9037512, source 10.229.53.91, destination 128.93.162.83, protocol ICMP, and length 106. The packet details pane shows the ICMP Echo (ping) request with ID 0x0001, sequence 59, and TTL 1. The packet bytes pane shows the raw data of the ICMP Echo request.

No.	Time	Source	Destination	Protocol	Length	Info
88	9.037512	10.229.53.91	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=1 (no response found!)

Packet details for packet 88:

- Frame 88: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{F773D61D-0000-0000-0000-000000000000}
- 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: 128.93.162.83
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xf7c3 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 59 (0x003b)
 - Sequence Number (LE): 15104 (0x3b00)
 - [No response seen]

Packet bytes (hex):

```

0000  f4 ce 46 a6 09 74 30 c9 ab c3 3a cb
0010  00 5c 63 5c 00 00 01 01 f3 54 0a e5
0020  a2 53 08 00 f7 c3 00 01 00 00 00 00
0030  00 00 00 00 00 00 00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00 00 00 00 00
0060  00 00 00 00 00 00 00 00 00 00 00 00
  
```

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

1048	65.08964/	10.229.53.91	128.93.162.83	ICMP	106 Echo (ping) request	id=0x0001, seq=104/26624, ttl=16 (reply in 1054)
1054	66.038242	128.93.162.83	10.229.53.91	ICMP	106 Echo (ping) reply	id=0x0001, seq=104/26624, ttl=45 (request in 1048)
1055	66.039597	10.229.53.91	128.93.162.83	ICMP	106 Echo (ping) request	id=0x0001, seq=105/26880, ttl=16 (no response found!)
1179	69.563310	10.229.53.91	128.93.162.83	ICMP	106 Echo (ping) request	id=0x0001, seq=106/27136, ttl=16 (reply in 1226)
1226	70.034196	128.93.162.83	10.229.53.91	ICMP	106 Echo (ping) reply	id=0x0001, seq=106/27136, ttl=45 (request in 1179)

> Frame 1054: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{F773D6}	0000	30 c9 ab c3 3a cb f4 ce	46 a6 09 74 08 00
> Ethernet II, Src: HewlettP_wire(a6:09:74 {f4:ce:a6:09:74}), Dst: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)	0010	00 5c ac ee 00 00 2d 01	7c c6 80 5d a2 53
> Internet Protocol Version 4, Src: 128.93.162.83, Dst: 10.229.53.91	0020	35 5b 00 00 ff 96 00 01	00 68 00 00 00 00 00
> Internet Control Message Protocol	0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00
Type: 0 (Echo (ping) reply)	0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00
Code: 0	0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00
Checksum: 0xff96 [correct]	0060	00 00 00 00 00 00 00 00	00 00
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 104 (0x0068)			
Sequence Number (LE): 26624 (0x6800)			
[Request frame: 1048]			
[Response time: 348.595 ms]			

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?

5106	103.915082	128.93.162.83	10.229.53.91	ICMP	106 Echo (ping) reply	id=0x0001, seq=152/38912, ttl=45 (request in 5001)
5113	104.516775	128.93.162.83	10.229.53.91	ICMP	106 Echo (ping) reply	id=0x0001, seq=153/39168, ttl=45 (request in 5046)
5156	105.951643	128.93.162.83	10.229.53.91	ICMP	106 Echo (ping) reply	id=0x0001, seq=154/39424, ttl=45 (request in 5093)

> Frame 5156: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{F773D6...}

> Ethernet II, Src: HewlettP_a6:09:74 (f4:ce:a6:09:74), Dst: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

> Internet Protocol Version 4, Src: 128.93.162.83, Dst: 10.229.53.91

√ Internet Control Message Protocol

Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xfff64 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 154 (0x009a)
Sequence Number (LE): 39424 (0x9a00)
[\[Request frame: 5093\]](#)
[Response time: 3660.350 ms]

√ Data (64 bytes)

Data: 00...
[Length: 64]

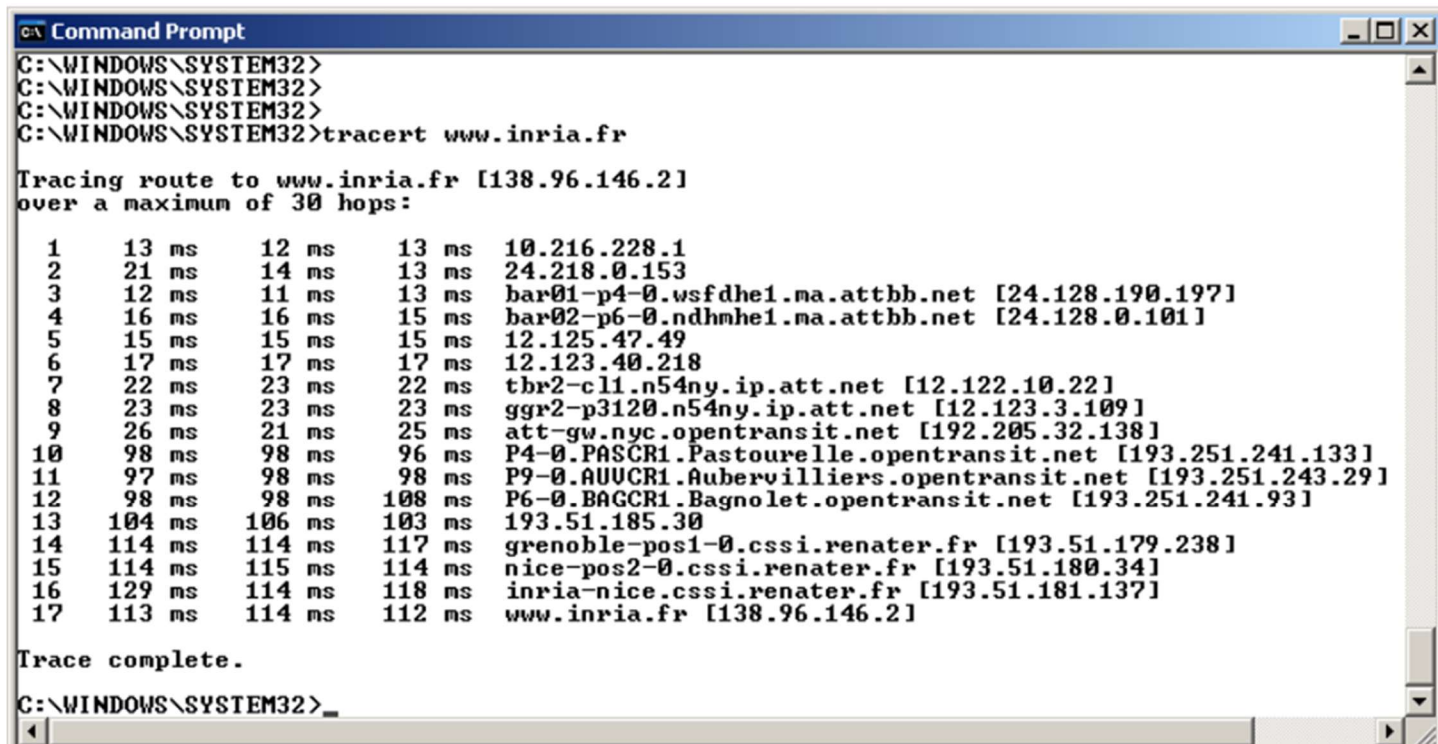
0000	30 c9 ab c3 3a cb f4 ce 46 a6 09 74
0010	00 5c 06 6e 00 00 2d 01 23 47 80 5d
0020	35 5b 00 00 ff 64 00 01 00 9a 00 00
0030	00 00 00 00 00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00 00 00 00 00 00

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 tracer 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:\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:
  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.wsfdhe1.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.PASCR1.Pastourelle.opentransit.net [193.251.241.133]
 10  97 ms  98 ms  98 ms  P9-0.AUUCR1.Aubervilliers.opentransit.net [193.251.243.29]
 11  98 ms  98 ms  108 ms  P6-0.BAGCR1.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>
```