

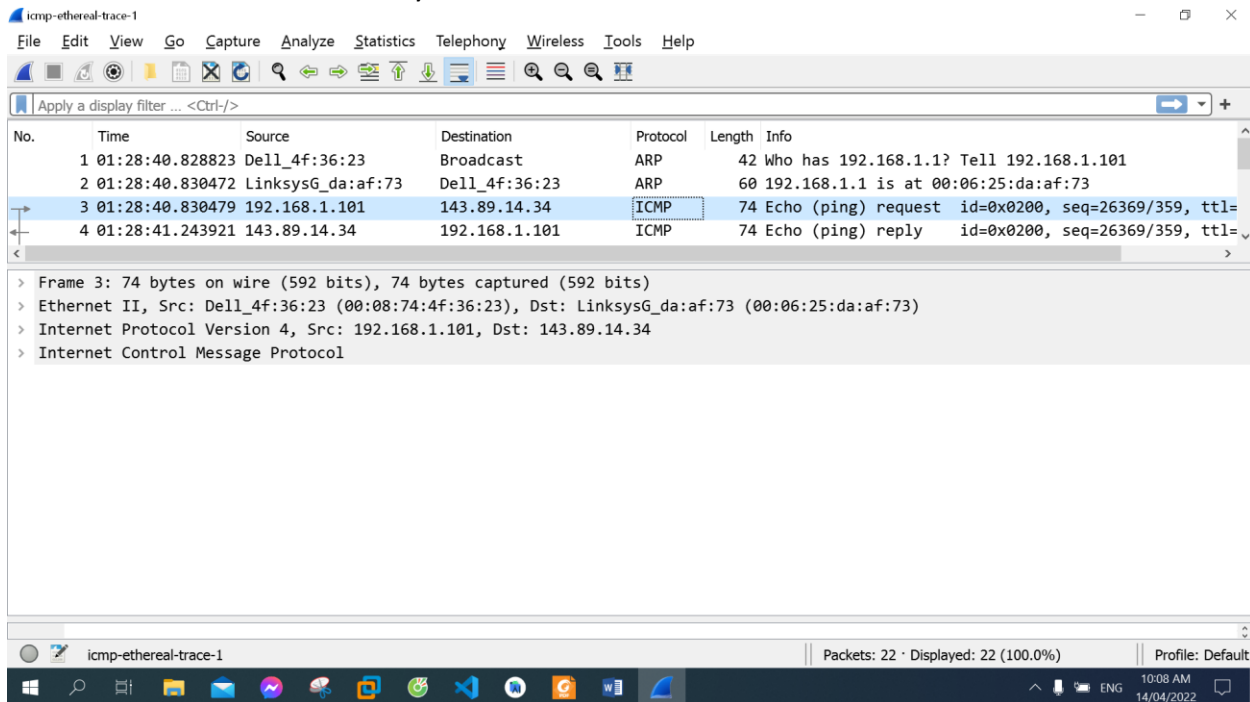
LAB 5

Wireshark Lab: ICMP v8.0

Name: Hồ Đức Trí

Student No: 1912288

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: 143.89.14.34

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.

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?

icmp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|-------------------|---------------|----------|--------|--|
| 1 | 01:28:40.828823 | Dell_4f:36:23 | Broadcast | ARP | 42 | Who has 192.168.1.1? Tell 192.168.1.101 |
| 2 | 01:28:40.830472 | LinksysG_da:af:73 | Dell_4f:36:23 | ARP | 60 | 192.168.1.1 is at 00:06:25:da:af:73 |
| 3 | 01:28:40.830479 | 192.168.1.101 | 143.89.14.34 | ICMP | 74 | Echo (ping) request id=0x0200, seq=26369/359, ttl= |
| 4 | 01:28:41.243921 | 143.89.14.34 | 192.168.1.101 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=26369/359, ttl= |

> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 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)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

icmp-ethereal-trace-1

Packets: 22 · Displayed: 22 (100.0%)

Profile: Default

10:10 AM 14/04/2022

ICMP type: 8

Code number: 0

Other fields this ICMP packet have: Checksum, Identifier, Sequence Number, Data
Each of them is 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?

icmp-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------------|-------------------|---------------|----------|--------|--|
| 1 | 01:28:40.828823 | Dell_4f:36:23 | Broadcast | ARP | 42 | Who has 192.168.1.1? Tell 192.168.1.101 |
| 2 | 01:28:40.830472 | LinksysG_da:af:73 | Dell_4f:36:23 | ARP | 60 | 192.168.1.1 is at 00:06:25:da:af:73 |
| 3 | 01:28:40.830479 | 192.168.1.101 | 143.89.14.34 | ICMP | 74 | Echo (ping) request id=0x0200, seq=26369/359, ttl= |
| 4 | 01:28:41.243921 | 143.89.14.34 | 192.168.1.101 | ICMP | 74 | Echo (ping) reply id=0x0200, seq=26369/359, ttl= |

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

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0xec5a [correct]

[Checksum Status: Good]

Identifier (BE): 512 (0x0200)

Identifier (LE): 2 (0x0002)

Sequence Number (BE): 26369 (0x6701)

Sequence Number (LE): 359 (0x0167)

[\[Request frame: 3\]](#)

[Response time: 413.442 ms]

Data (32 bytes)

Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

[Length: 32]

icmp-ethereal-trace-1

Packets: 22 · Displayed: 22 (100.0%)

Profile: Default

10:29 AM 14/04/2022

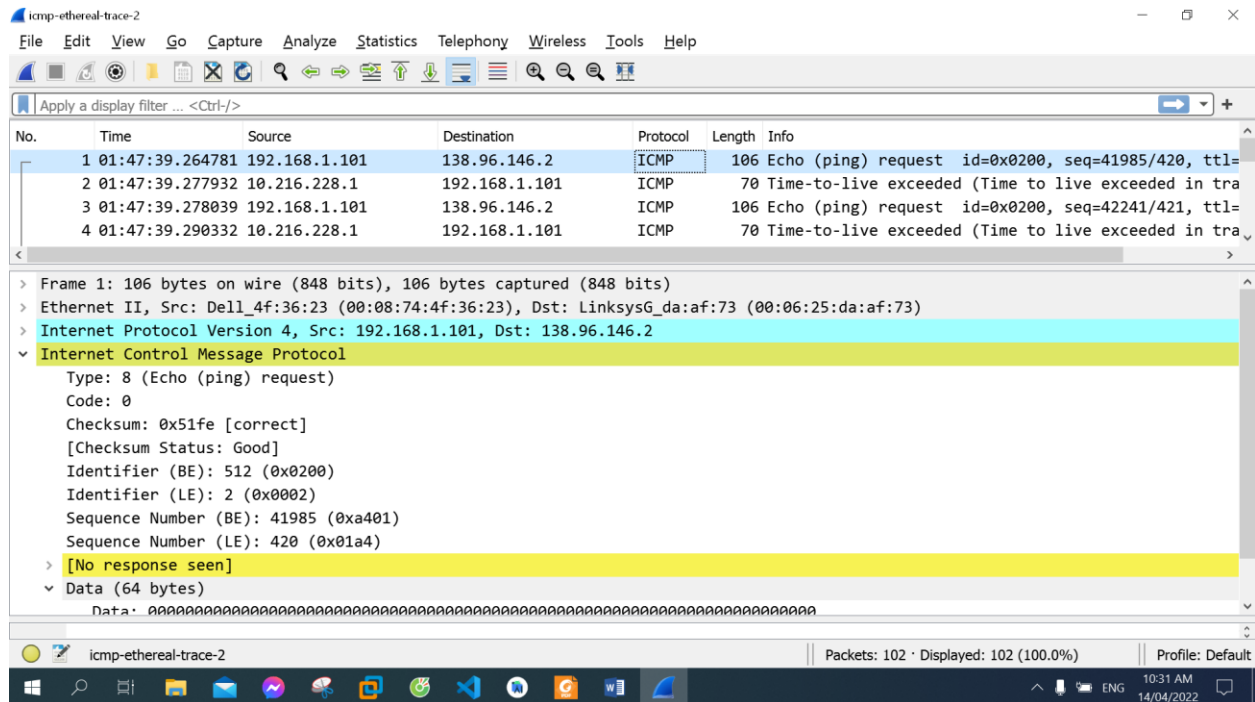
ICMP type: 0

Code number: 0

Other fields this ICMP packet have: Checksum, Identifier, Sequence Number, Data

Each of them is 2 bytes

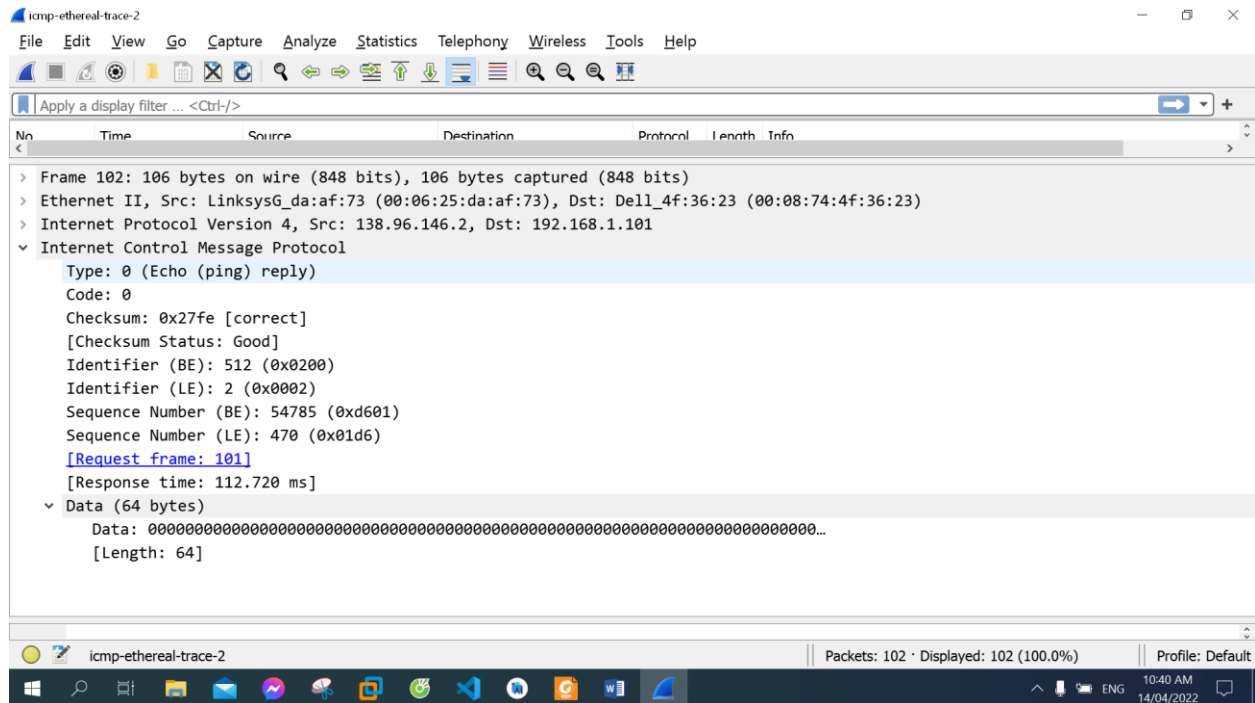
5. What is the IP address of your host? What is the IP address of the target destination host?



The IP address of my host: 192.168.1.101

The IP address of the target destination: 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, the IP protocol number 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?
They have same fields, same ICMP type (8) and code number (0)
8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?



These packets have ICMP type = 0 while the error packets have ICMP type = 11, they have Response frame and Response time, they do not have IPv4 fields and information of the packet that was in error.

They are different because the destination host receive them successfully within the TTL.

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?

```

Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

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

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

 1  *      *      *      Request timed out.
 2  7 ms    7 ms    7 ms    125.235.249.190.adsl.viettel.vn [125.235.249.190]
 3  9 ms    13 ms   11 ms    10.255.40.155
 4  6 ms    6 ms    19 ms    DESKTOP-8S8N8IR [27.68.237.186]
 5  40 ms   37 ms   36 ms    DESKTOP-8S8N8IR [27.68.237.139]
 6  28 ms   27 ms   43 ms    DESKTOP-8S8N8IR [27.68.250.169]
 7  35 ms   28 ms   44 ms    xe-2-2-3-xcr1.hke.cw.net [195.89.113.21]
 8  53 ms   178 ms  194 ms    ae4-xcr1.hkg.cw.net [195.2.10.97]
 9  190 ms  188 ms  177 ms    ae11-xcr1.lax.cw.net [195.2.8.33]
10  181 ms  266 ms  187 ms    gtt-gw.lax.cw.net [195.2.14.46]
11  317 ms  314 ms  314 ms    et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
12  228 ms  226 ms  230 ms    renater-gw-ix1.gtt.net [77.67.123.206]
13  228 ms  234 ms  230 ms    te1-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
14  245 ms  235 ms  226 ms    inria-rocquencourt-gi3-2-inria-rtr-021.noc.renater.fr [193.51.184.177]
15  228 ms  228 ms  226 ms    unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
16  230 ms  230 ms  239 ms    prod-inriafr-cms.inria.fr [128.93.162.83]

Trace complete.

C:\Users\THINKPAD>

```

There are 2 links whose delay are significantly longer than others, between 7 and 8, between 10 and 11

```

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    thr2-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.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>

```

Refer to the screenshot in Figure 4, there is a link whose delay is significantly longer than others, between 9 and 10

In figure 4 from the lab, the link is from New York to France