CISC 335 – Computer Networks – Winter 2021
Wireshark Assignment 2: ICMP

Due April 2, 2021, 11:59 pm

Objective

This lab assignment aims to make you explore the following operations of the ICMP protocol:

- A Ping operation.
- A Traceroute operation.

Tools:

The employed tools in this lab are:

- Command Prompt in Windows OS, or Terminal in either MAC OS or Linux.
- Wireshark Network Analyzer.

Lab Report Instruction

The lab report should include:

- A screen shot of the designated screens where requested.
- An answer to each question in its numbered position within the assignment.

When answering a question, you should hand in a <u>printout or a screenshot</u> of the packet(s) within the trace that you used to answer the question asked. Annotate the <u>printout or screenshot</u> to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question (or take a screenshot showing this minimum amount of packet detail).

Experiment 1: Examining the ICMP Messages of a Ping Operation

In this experiment, you will observe the ICMP protocol in action when a ping operation is being executed. The steps of this experiment are as follows for Windows OS (Hints: they will be given **<u>for MAC and Linux between parenthesis</u>**, but please check the corresponding commands online if needed):

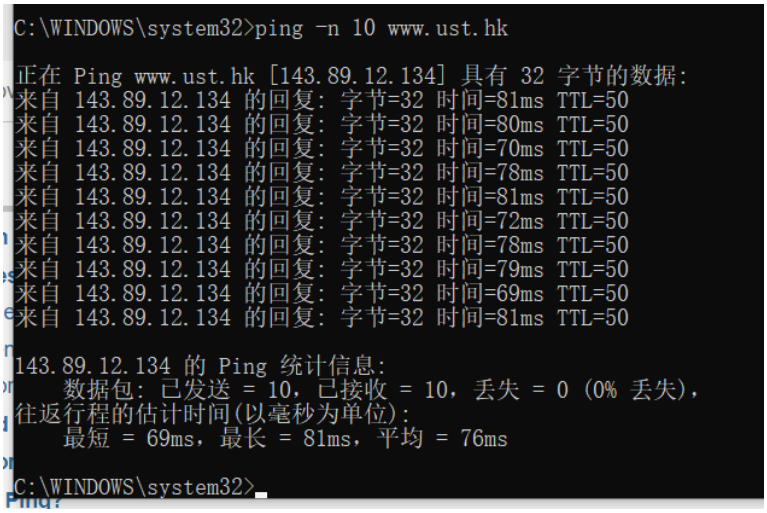
- Open the Command Prompt and Choose "Run as Administrator" (For MAC OS and Linux, just open the Terminal).
- Open Wireshark and start capturing on your employed network interface.
- Go back to the Command Prompt (or Terminal) and type `ping -n 10` www.ust.hk
    - or `c:\windows\system32\ping -n 10` www.ust.hk
    - (`ping -c 10` www.ust.hk in Terminal). The number 10 specifies that 10 ping messages will be sent.

- Observe the progression of displayed information in the Command Prompt (Terminal). When the ping process is terminated, stop the packet capture in Wireshark.

Now, please answer the following:

1. Provide a screenshot of the information displayed in the Command Prompt (Terminal). What is the round-trip time (RTT) of the first 5 packets of the ping process?

Sorry about this, but my PC's operating system is of Chinese language.



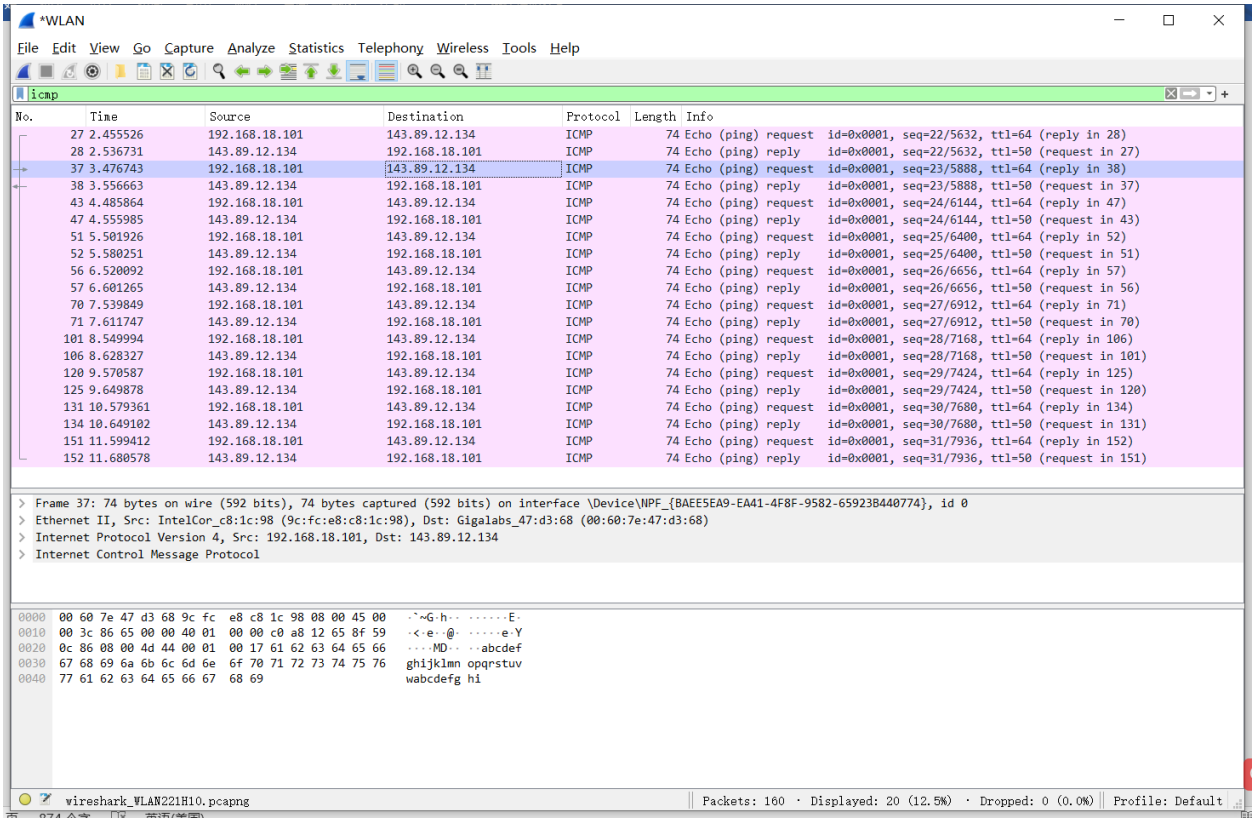
```
C:\WINDOWS\system32>ping -n 10 www.ust.hk

正在 Ping www.ust.hk [143.89.12.134] 具有 32 字节的数据:
来自 143.89.12.134 的回复: 字节=32 时间=81ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=80ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=70ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=78ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=81ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=72ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=78ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=79ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=69ms TTL=50
来自 143.89.12.134 的回复: 字节=32 时间=81ms TTL=50

143.89.12.134 的 Ping 统计信息:
    数据包: 已发送 = 10，已接收 = 10，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 69ms，最长 = 81ms，平均 = 76ms

C:\WINDOWS\system32>
```

Round-trip time (RTT) of the first 5 packets of the ping process:

Total: 390ms

Average: 78ms

2. Go to Wireshark, filter ICMP packets, and capture a screenshot of the result.

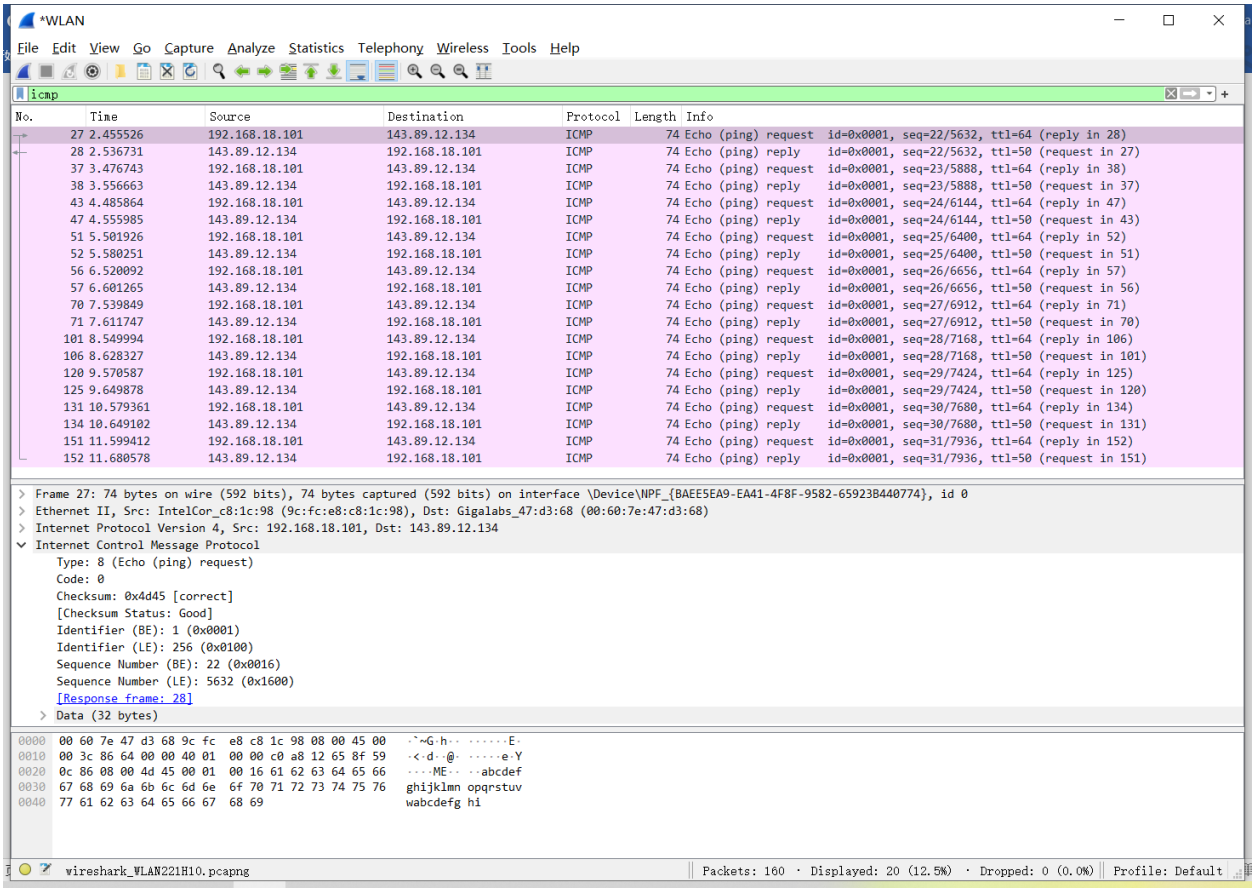


3. What is the source and destination IP addresses of the ICMP ping process?

When an ICMP request was sent out, the source is 192.168.18.101, and the destination is 143.89.12.134.

When an ICMP reply was received, the source is 143.89.12.134, and the destination is 192.168.18.101.

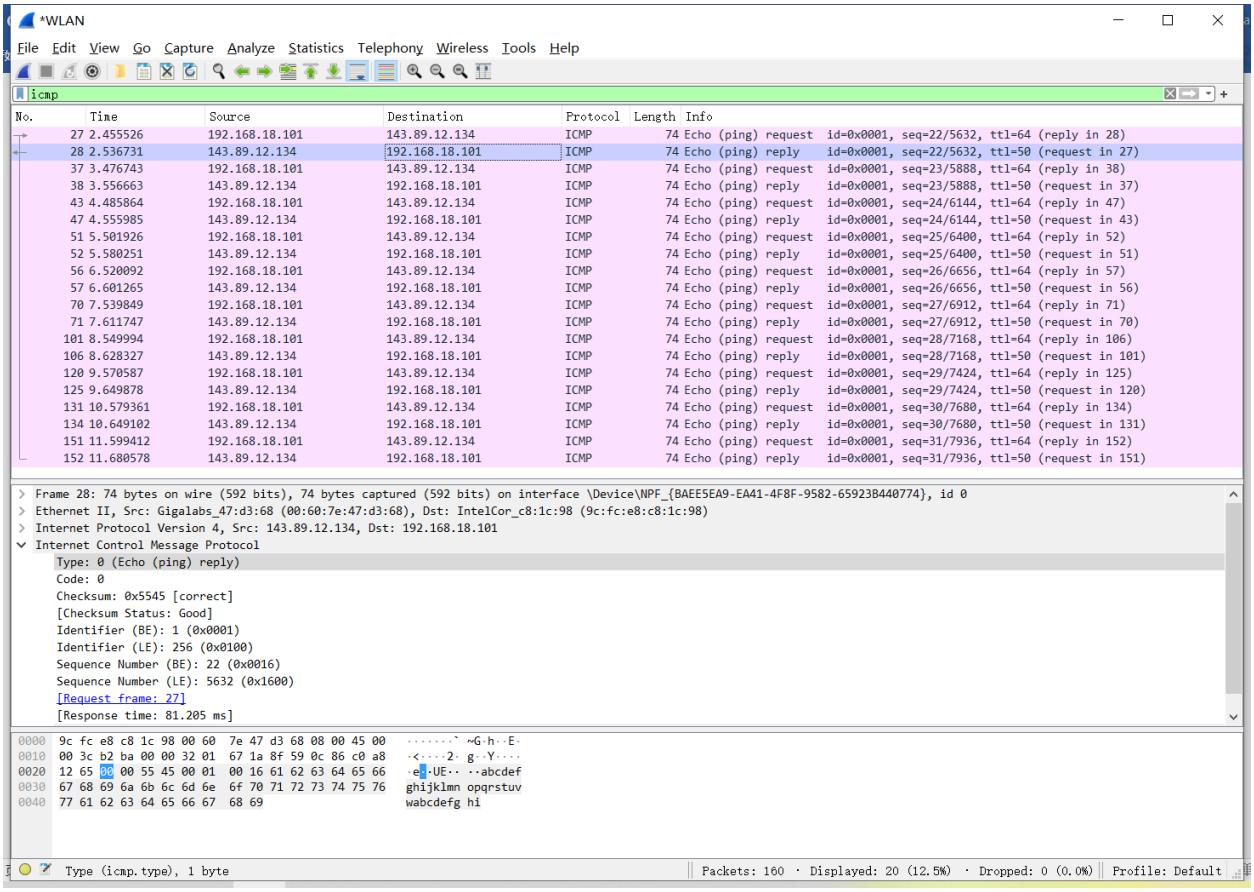
4. Examine one of the ICMP request packets. Provide a screenshot for the upper, middle, and lower windows. What are the ICMP type and code numbers? What other fields does this ICMP packet have?



The ICMP type is: 8 (Echo (ping) request). **The code numbers are:** 0

Other fields that this ICMP packet have include: checksum, identifier (BE), identifier (LE), sequence number (BE), sequence number (LE), as shown in the above screenshot.

5. Examine the corresponding ping reply of the request examined in part 4. Provide a screenshot for the upper, middle, and lower windows. What are the ICMP type and code numbers? What other fields does this ICMP packet have?



The ICMP type is: 0 (Echo (ping) reply). **The code numbers are:** 0

Other fields that this ICMP packet have include: checksum, identifier (BE), identifier (LE), sequence number (BE), sequence number (LE), as shown in the above screenshot.

Experiment 2: Examining the ICMP Messages of a Traceroute Operation

In this experiment, you will observe the ICMP protocol in action when a traceroute operation is being executed. The steps of this experiments are as follows for Windows OS (Hints will be given **for MAC and Linux between parenthesis**, but please check the corresponding commands online if needed):

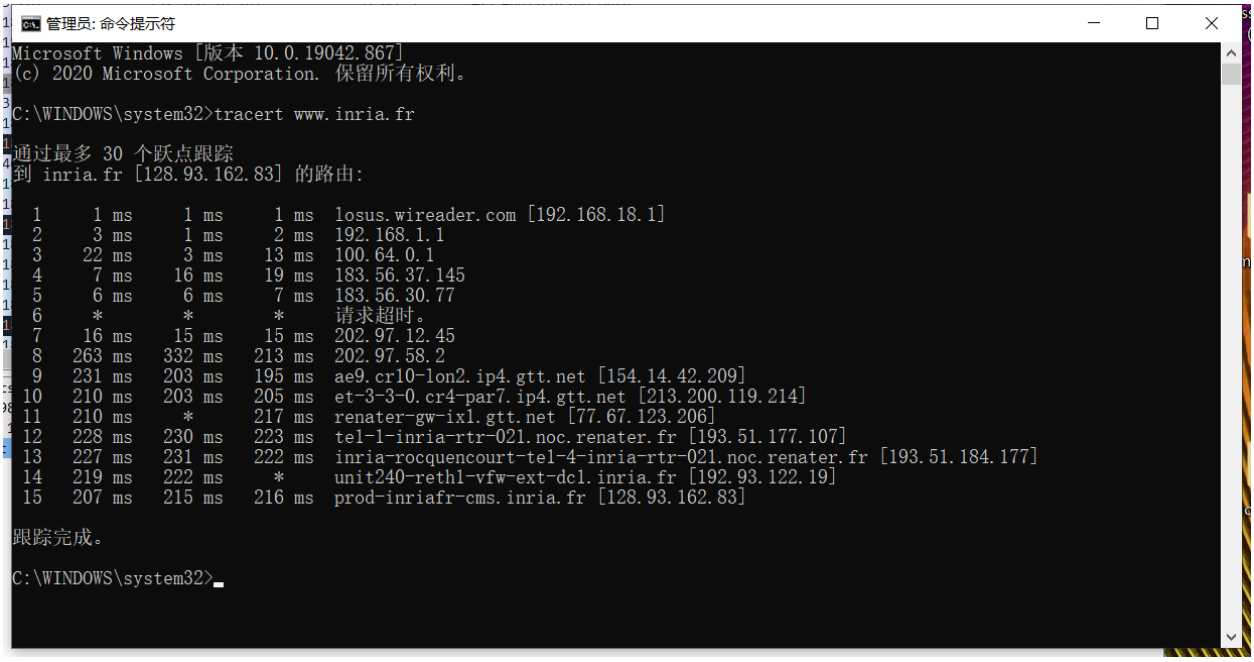
- Open the Command Prompt and Choose "Run as Administrator" (For MAC OS and Linux, just open the Terminal).
- Open Wireshark and start capturing on your employed network interface.
- Go back to the Command Prompt (or Terminal) and type `tracert www.inria.fr` or `c:\windows\system32\tracert www.inria.fr` (`traceroute www.inria.fr` in Terminal). (If the traceroute process to the above address was not successful, try `www.u-tokyo.ac.jp` then `www.epfl.ch`)

- Observe the progression of displayed information in the Command Prompt (Terminal). When the traceroute process is terminated, stop the packet capture in Wireshark.

Now, please answer the following:

1. Provide a screenshot of the information displayed in the Command Prompt (Terminal). What is the number of links between the source and destination?

Sorry about this, but my PC's operating system is of Chinese language.



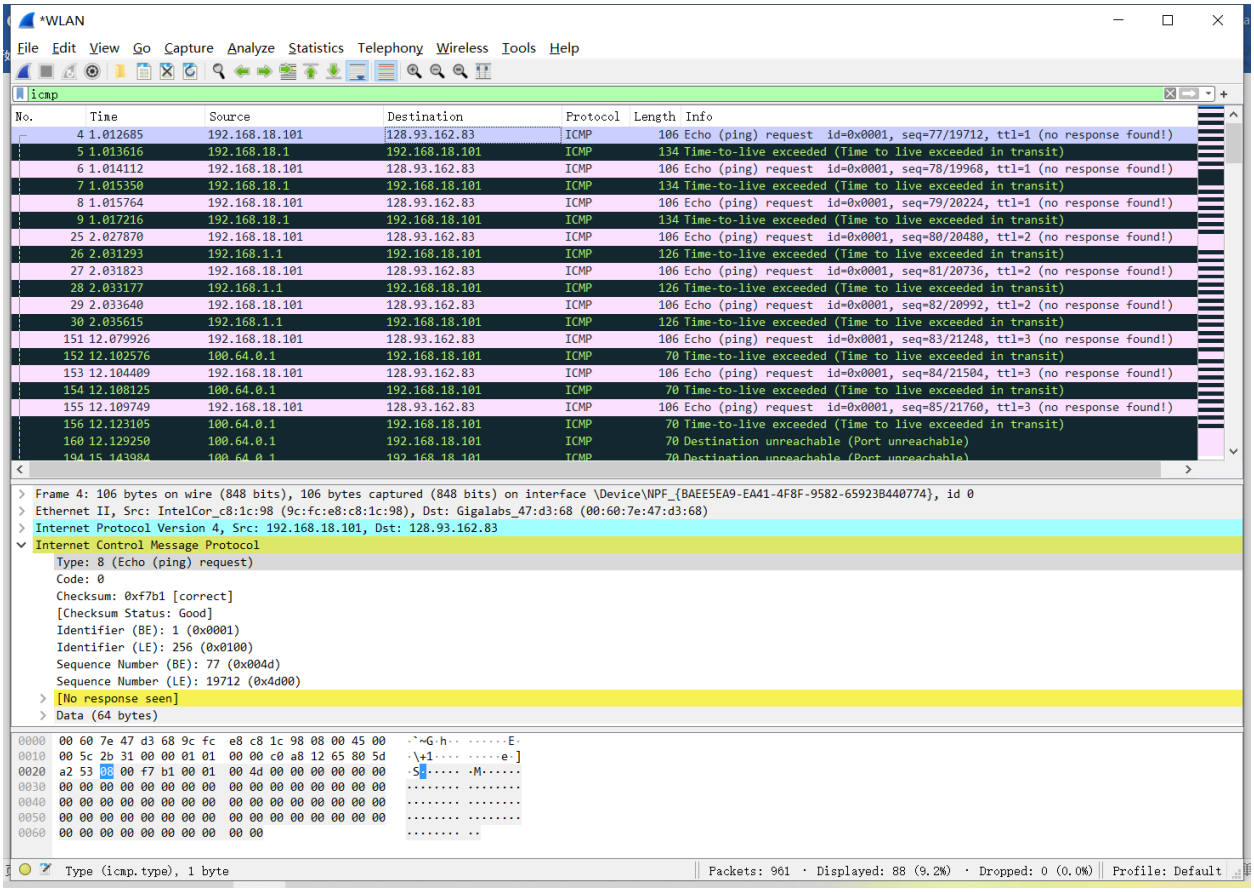
```
管理员: 命令提示符
Microsoft Windows [版本 10.0.19042.867]
(c) 2020 Microsoft Corporation. 保留所有权利。

C:\WINDOWS\system32>tracert www.inria.fr

通过最多 30 个跃点跟踪
到 inria.fr [128.93.162.83] 的路由:

  1     1 ms     1 ms     1 ms  losus.wireader.com [192.168.18.1]
  2     3 ms     1 ms     2 ms  192.168.1.1
  3    22 ms     3 ms    13 ms  100.64.0.1
  4     7 ms    16 ms    19 ms  183.56.37.145
  5     6 ms     6 ms     7 ms  183.56.30.77
  6     *        *        *     请求超时。
  7    16 ms    15 ms    15 ms  202.97.12.45
  8   263 ms   332 ms   213 ms  202.97.58.2
  9   231 ms   203 ms   195 ms  ae9.cr10-lon2.ip4.gtt.net [154.14.42.209]
 10   210 ms   203 ms   205 ms  et-3-3-0.cr4-par7.ip4.gtt.net [213.200.119.214]
 11   210 ms     *      217 ms  renater-gw-ix1.gtt.net [77.67.123.206]
 12   228 ms   230 ms   223 ms  tel-1-inria-rtr-021.noc.renater.fr [193.51.177.107]
 13   227 ms   231 ms   222 ms  inria-rocquencourt-tel-4-inria-rtr-021.noc.renater.fr [193.51.184.177]
 14   219 ms   222 ms     *     unit240-reth1-vfw-ext-dc1.inria.fr [192.93.122.19]
 15   207 ms   215 ms   216 ms  prod-inriafr-cms.inria.fr [128.93.162.83]

跟踪完成。

C:\WINDOWS\system32>
```

The number of links between source and destination is: 15

2. From the command prompt (or terminal), what is the IP address of the router rendering the highest round-trip time (RTT). Note that traceroute provides the round-trip time for each hop in milliseconds (ms). Three different times are provided for each hop since three separate probe requests are sent by default for each hop. In this question, consider the highest RTT based on the third reported number in each link.

IP address of the router rendering the highest round-trip time (RTT) is: 193.51.177.107

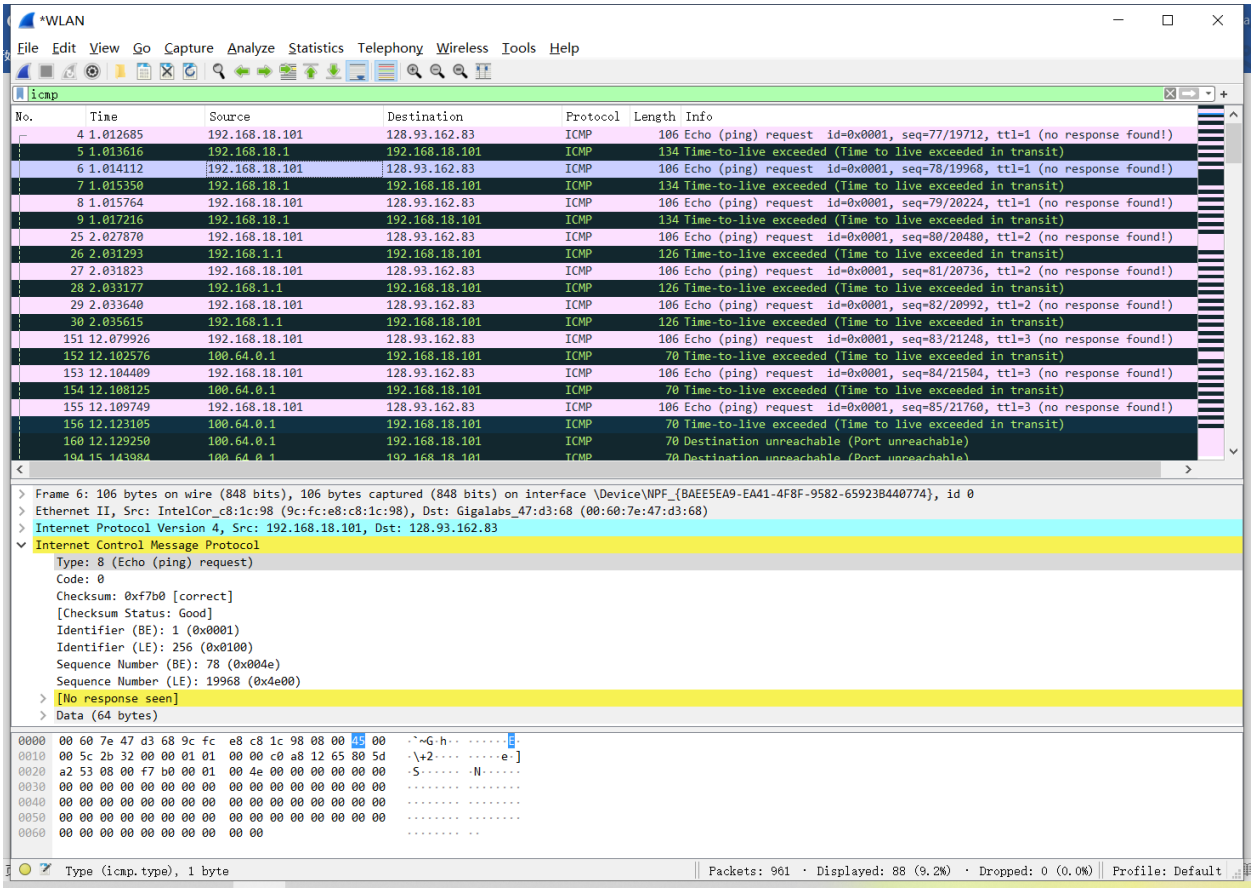
3. Go to Wireshark, filter ICMP packets, and capture a screenshot of the result. What is the IP address of your host? What is the IP address of the final destination host?



The IP address of my host is: 192.168.18.101

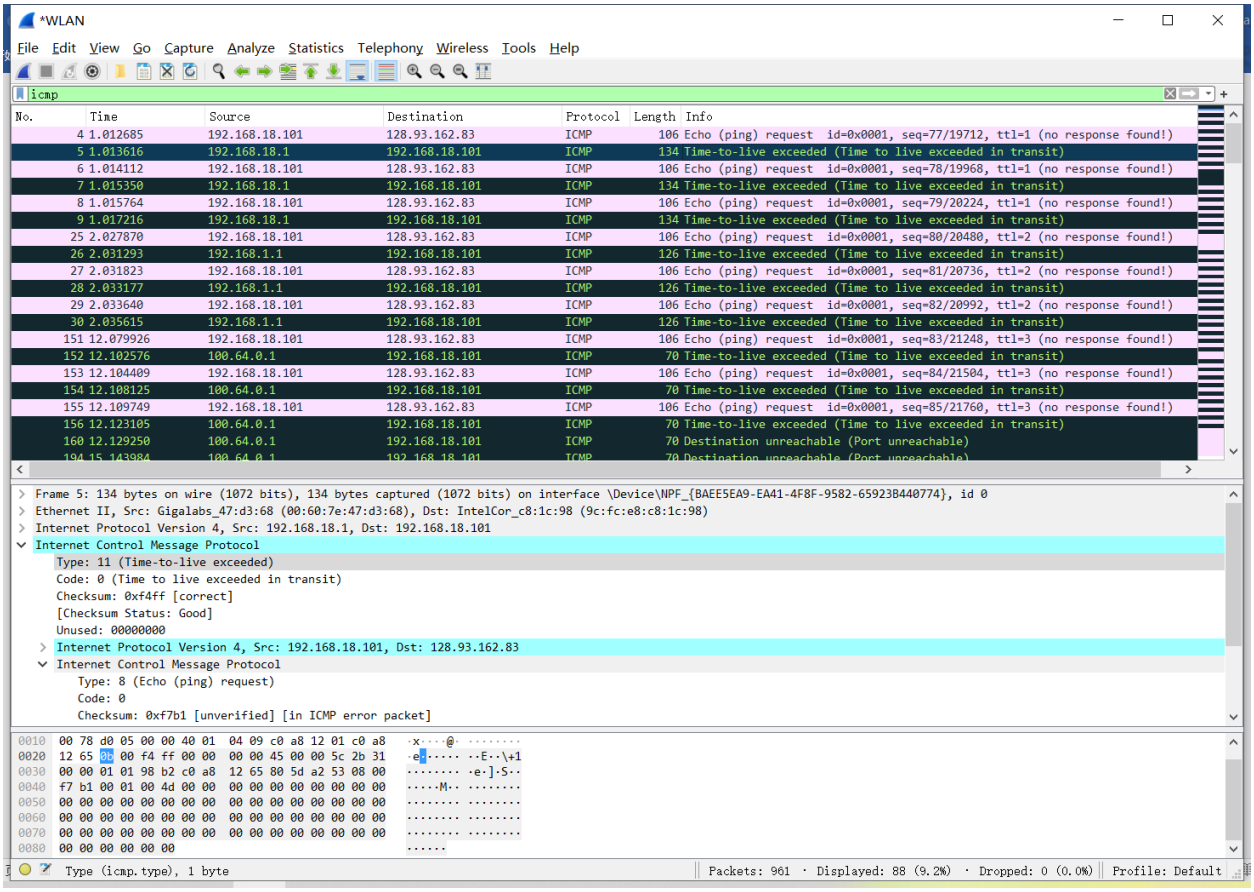
The IP address of the final destination host is: 128.93.162.83

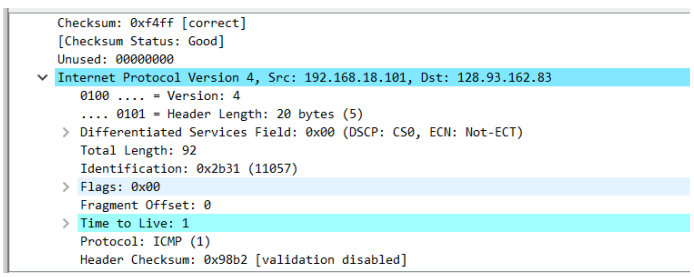
4. Examine one of the early ICMP echo packets (e.g., 2nd or 3rd). Is this packet different from the ICMP ping query packets in Experiment 1 of this assignment? (Hint: Compare the fields).



This packet is different from the ICMP ping query packets in Experiment 1 of this assignment, in the sense that there's *no response seen*, which was highlighted in yellow in the above screenshot. Other fields are likely quite similar to those we've seen in Experiment 1.

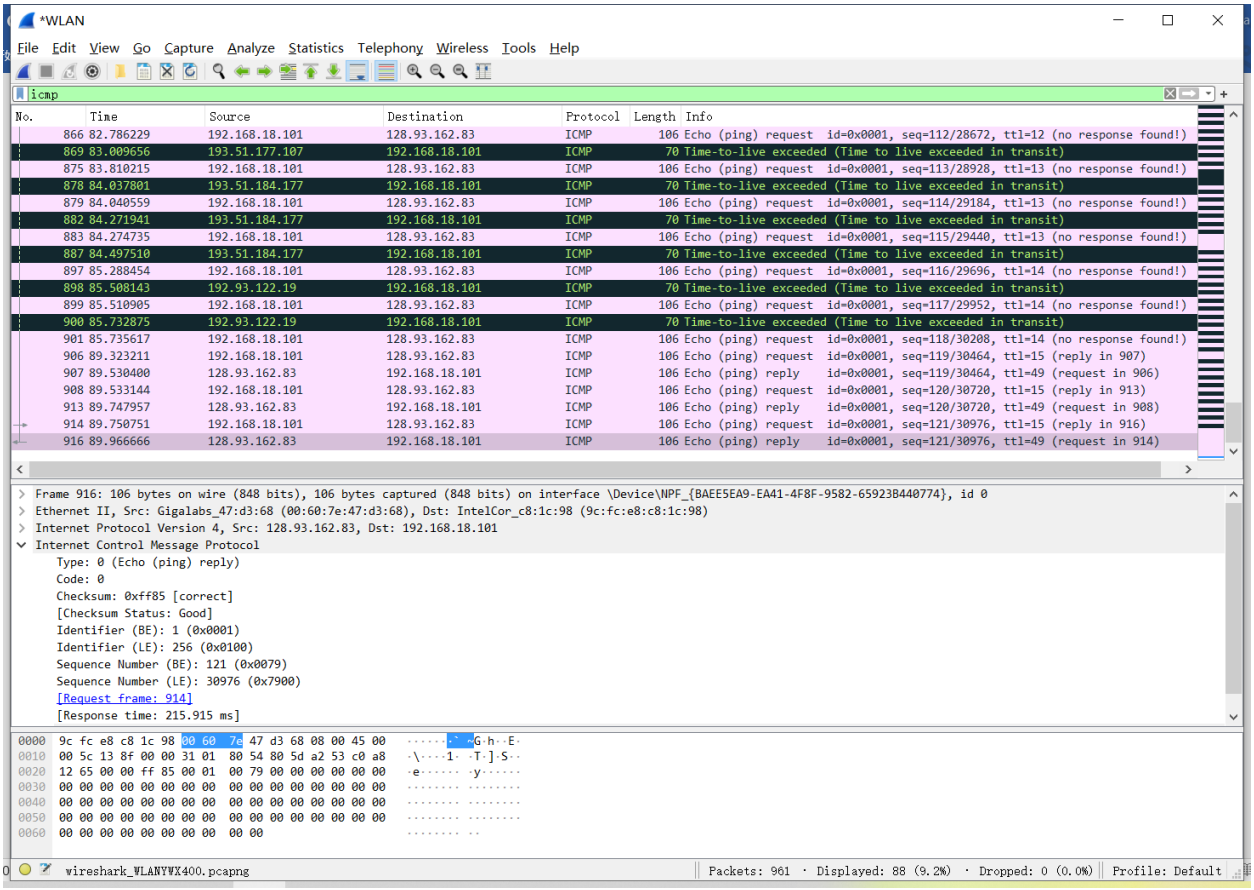
5. Examine the ICMP error packet corresponding to the ICMP echo packet examined in Step 3. What is the indicated error? The packet should have additional fields than the ICMP echo packet. What is included in those fields? (Hint: When you expand the ICMP details in the middle window, report what you see).





The indicated error is a timed-out error. The packet should have additional fields than the ICMP echo packet. There are two ICMP rows in the detail here. As I expand the ICMP details in the middle window, I could see that the 'Time to Live' field is set to 1 here, as shown in the above screenshot, highlighted as blue. The type is of 11 indicating that there's an error where time-to-live exceeded.

6. Examine the last three ICMP packets received by the source. How are these packets different from the ICMP error packets? Why are they different? (Hint: compare the type and code fields and provide an explanation accordingly).



These packets were different from the ICMP error packets, in the sense that there were no timed-out errors happening here, and that a ICMP reply is followed by a ICMP request, just like experiment 1.

They were different because this time the type field is: 0 (Echo (ping) reply), and the code field is: 0.

However, the type field from step 5 is: 11, indicating an error where time-to-live exceeded. But then now the last three ICMP packets received by the source contain no errors.