

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 printout or a screenshot of the packet(s) within the trace that you used to answer the question asked. Annotate the printout or screenshot 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 **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 `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.

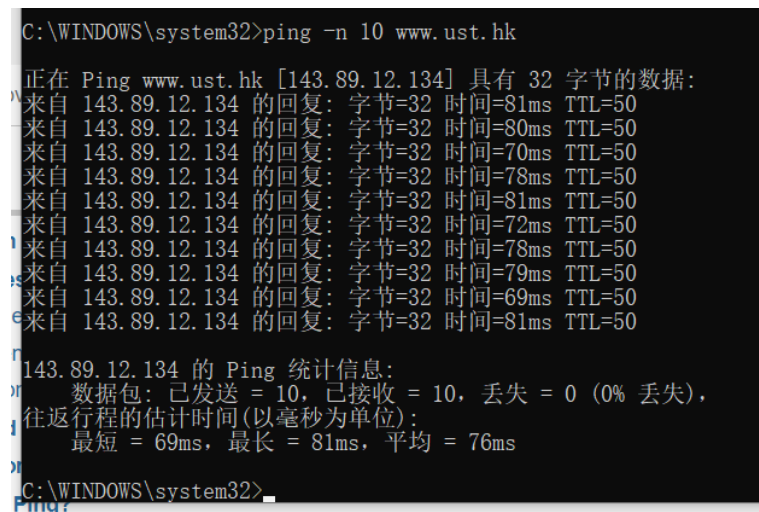
- Observe the progression of displayed information in the Command Prompt (Terminal). When the ping process is terminated, stop the packet capture in Wireshark.

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

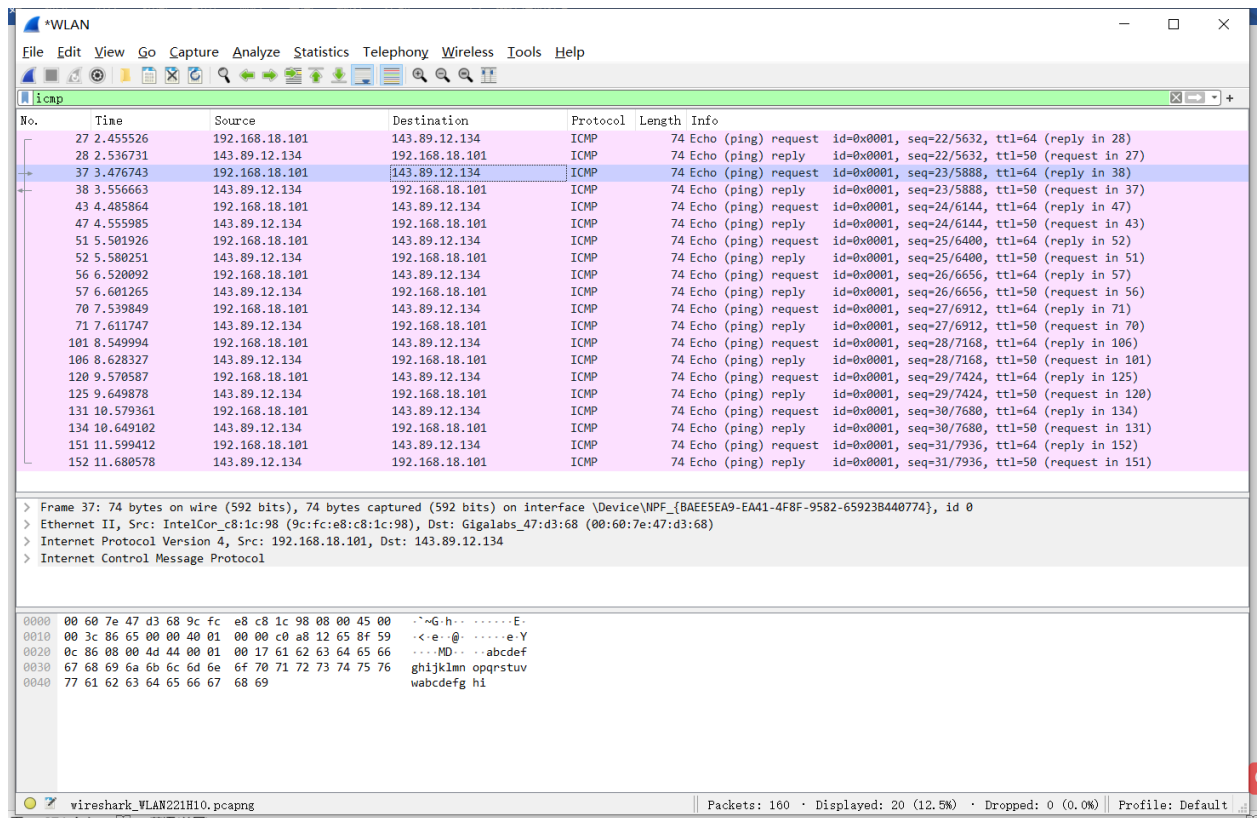
C:\WINDOWS\system32>
```

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?

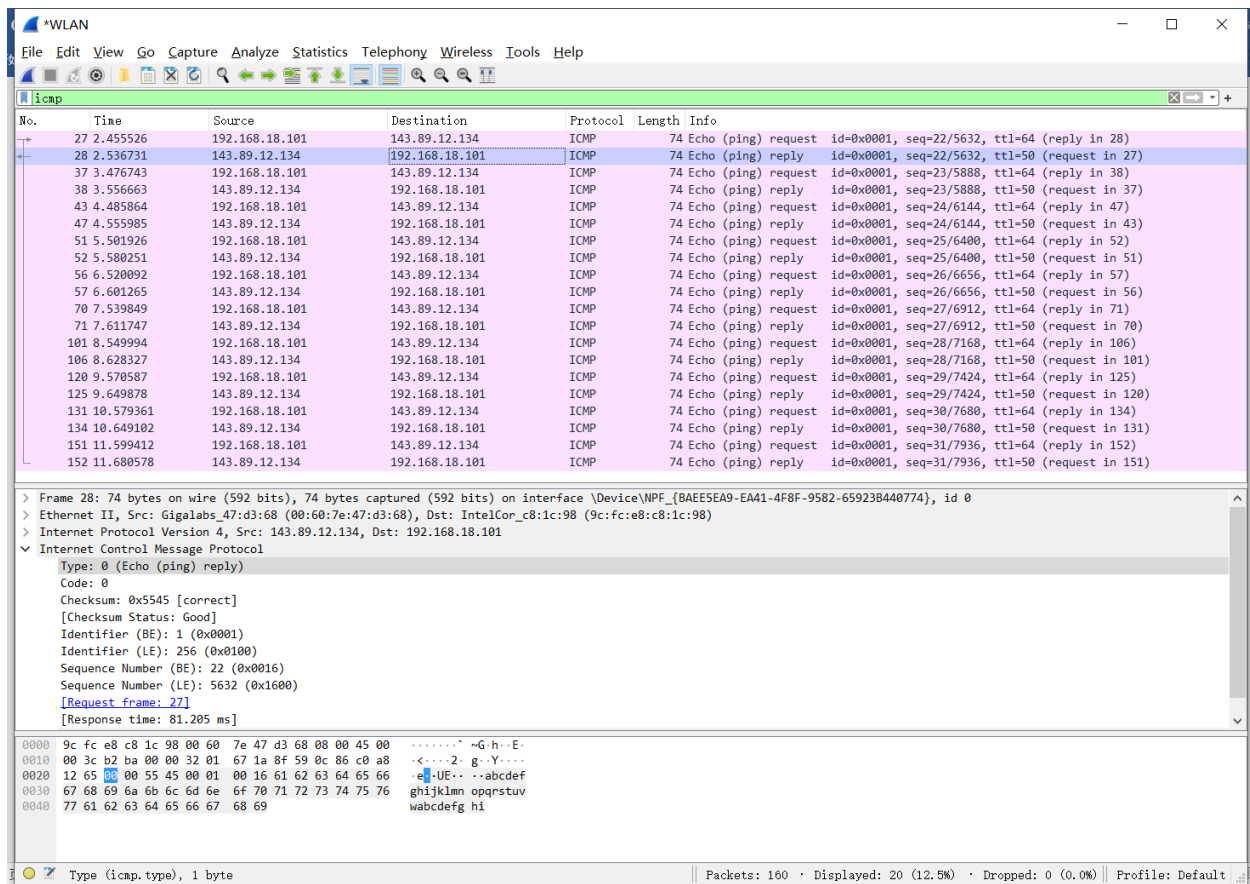
No.	Time	Source	Destination	Protocol	Length	Info
27	2.455526	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (reply in 28)
28	2.536731	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=22/5632, ttl=50 (request in 27)
37	3.476743	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=23/5888, ttl=64 (reply in 38)
38	3.556663	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=23/5888, ttl=50 (request in 37)
43	4.485864	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=24/6144, ttl=64 (reply in 47)
47	4.555985	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=50 (request in 43)
51	5.501926	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=64 (reply in 52)
52	5.580251	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=50 (request in 51)
56	6.520092	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=64 (reply in 57)
57	6.601265	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=50 (request in 56)
70	7.539849	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=64 (reply in 71)
71	7.611747	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=50 (request in 70)
101	8.549994	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=64 (reply in 106)
106	8.628327	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=50 (request in 101)
120	9.570587	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=64 (reply in 125)
125	9.649878	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=50 (request in 120)
131	10.579361	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=64 (reply in 134)
134	10.649102	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=50 (request in 131)
151	11.599412	192.168.18.101	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=64 (reply in 152)
152	11.680578	143.89.12.134	192.168.18.101	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=50 (request in 151)

> Frame 27: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{BAEE5EA9-EA41-4F8F-9582-65923B440774}, id 0
 > Ethernet II, Src: IntelCon_c8:1c:98 (9c:fc:e8:c8:1c:98), Dst: Gigalabs_47:d3:68 (00:60:7e:47:d3:68)
 > Internet Protocol Version 4, Src: 192.168.18.101, Dst: 143.89.12.134
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4d45 [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence Number (BE): 22 (0x0016)
 Sequence Number (LE): 5632 (0x1600)
 [Response frame: 28]
 Data (32 bytes)
 0000 00 60 7e 47 d3 68 9c fc e8 c8 1c 98 08 00 45 00 ..>G-h...-...E
 0010 00 3c 86 64 00 00 40 01 00 00 c0 a8 12 65 8f 59 <-d-@-...e-Y
 0020 0c 86 08 00 4d 45 00 01 00 16 61 62 63 64 65 66 ...ME...abcdef
 0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
 0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

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.

- 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)

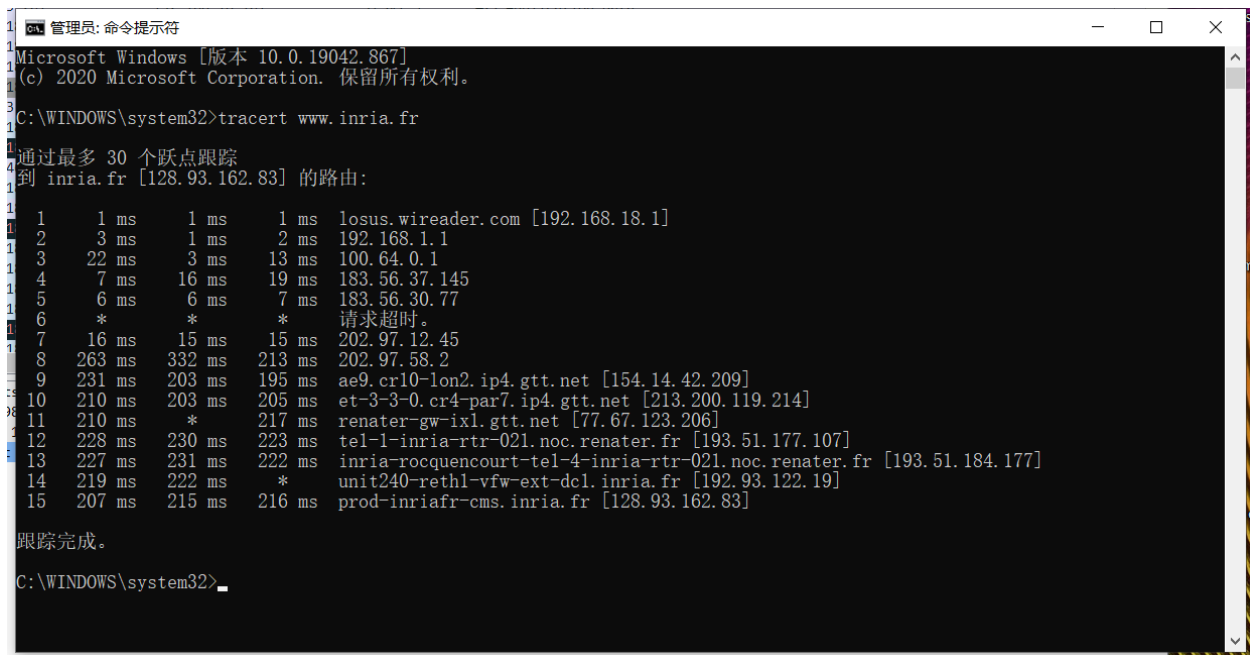
- Observe the progression of displayed information in the Command Prompt (Terminal). When the traceroute process is terminated, stop the packet capture in Wireshark.

Now, please answer the following:

- 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-ixl.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-dcl.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

- 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

- 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 screenshot shows a Wireshark packet capture on the 'icmp' filter. The packet list shows ICMP Echo (ping) requests from source 192.168.18.101 to destination 128.93.162.83. The information pane for the selected packet (No. 4) shows the following details:

- Frame 4: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BAEE5EA9-EA41-4F8F-9582-65923B440774}, id 0
- Ethernet II, Src: IntelCon_c8:1c:98 (9c:fc:e8:c8:1c:98), Dst: Gigalabs_47:d3:68 (00:60:7e:47:d3:68)
- Internet Protocol Version 4, Src: 192.168.18.101, Dst: 128.93.162.83
- Internet Control Message Protocol
 - Type: 8 (Echo (ping) request)
 - Code: 0
 - Checksum: 0xf7b1 [correct]
 - [Checksum Status: Good]
 - Identifier (BE): 1 (0x0001)
 - Identifier (LE): 256 (0x0100)
 - Sequence Number (BE): 77 (0x004d)
 - Sequence Number (LE): 19712 (0x4d00)
- [No response seen]
- Data (64 bytes)

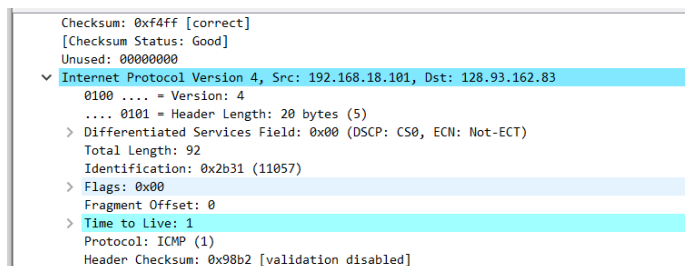
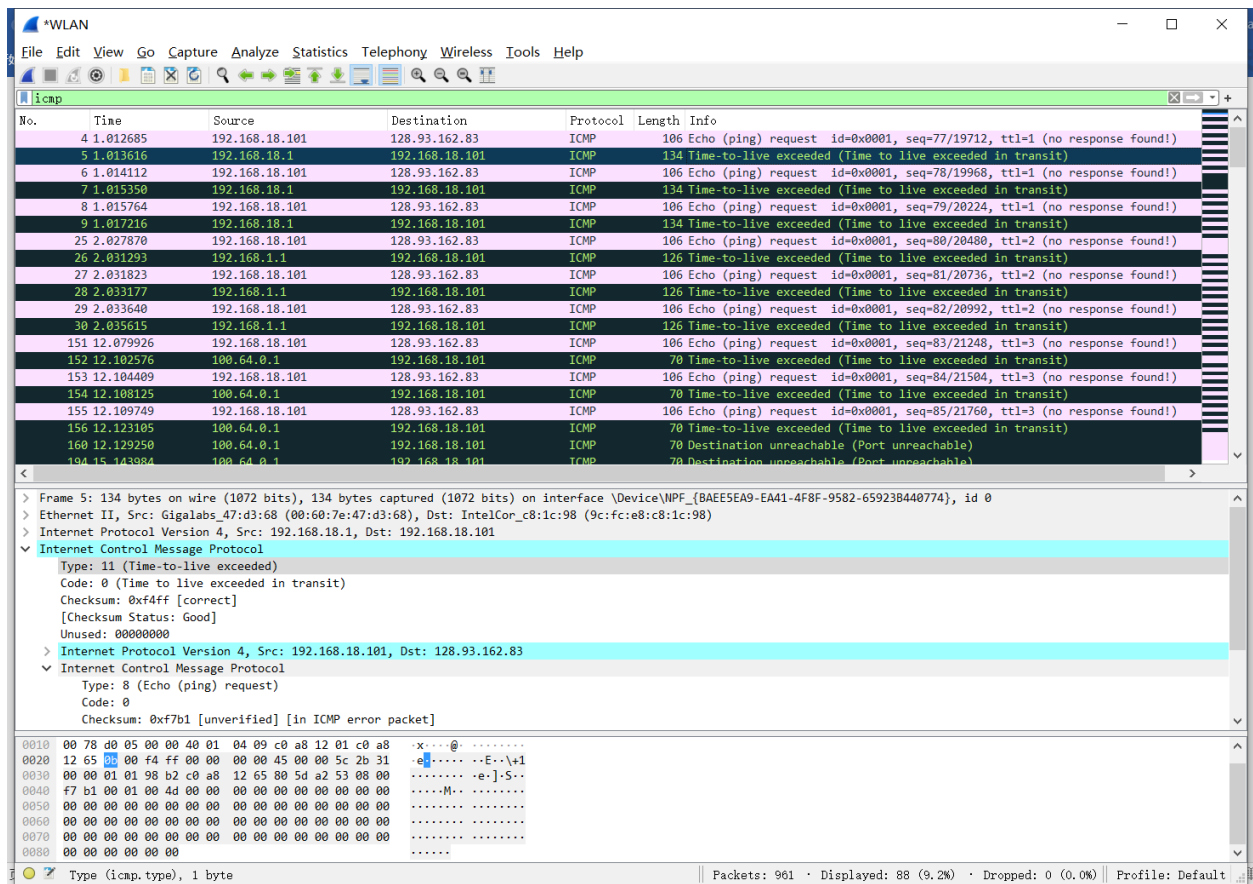
The packet bytes pane shows the raw data of the ICMP Echo request, including the header and the 64-byte data payload.

The IP address of my host is: 192.168.18.101

The IP address of the final destination host is: 128.93.162.83

- 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).

- 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.

- 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).

No.	Time	Source	Destination	Protocol	Length	Info
866	82.786229	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=112/28672, ttl=12 (no response found!)
869	83.009656	192.51.177.107	192.168.18.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
875	83.810215	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=113/28928, ttl=13 (no response found!)
878	84.037801	192.51.184.177	192.168.18.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
879	84.040559	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=114/29184, ttl=13 (no response found!)
882	84.271941	192.51.184.177	192.168.18.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
883	84.274735	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=115/29440, ttl=13 (no response found!)
887	84.497510	192.51.184.177	192.168.18.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
897	85.288454	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=116/29696, ttl=14 (no response found!)
898	85.508143	192.93.122.19	192.168.18.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
899	85.510905	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=117/29952, ttl=14 (no response found!)
900	85.732875	192.93.122.19	192.168.18.101	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
901	85.735617	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=118/30208, ttl=14 (no response found!)
906	89.323211	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=119/30464, ttl=15 (reply in 907)
907	89.530400	128.93.162.83	192.168.18.101	ICMP	106	Echo (ping) reply id=0x0001, seq=119/30464, ttl=49 (request in 906)
908	89.533144	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=120/30720, ttl=15 (reply in 913)
913	89.747957	128.93.162.83	192.168.18.101	ICMP	106	Echo (ping) reply id=0x0001, seq=120/30720, ttl=49 (request in 908)
914	89.750751	192.168.18.101	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=121/30976, ttl=15 (reply in 916)
916	89.966666	128.93.162.83	192.168.18.101	ICMP	106	Echo (ping) reply id=0x0001, seq=121/30976, ttl=49 (request in 914)

> Frame 916: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{BAE5EA9-EA41-4F8F-9582-65923B440774}, id 0	
> Ethernet II, Src: Gigalabs_47:d3:68 (00:60:7e:47:d3:68), Dst: IntelCor_8:1c:98 (9c:fc:e8:c8:1c:98)	
> Internet Protocol Version 4, Src: 128.93.162.83, Dst: 192.168.18.101	
▼ Internet Control Message Protocol	
Type: 0 (Echo (ping) reply)	
Code: 0	
Checksum: 0xff85 [correct]	
[Checksum Status: Good]	
Identifier (BE): 1 (0x0001)	
Identifier (LE): 256 (0x0100)	
Sequence Number (BE): 121 (0x0079)	
Sequence Number (LE): 30976 (0x7900)	
[Request frame: 914]	
[Response time: 215.915 ms]	

0000	9c fc e8 c8 1c 98 00 60 7e 47 d3 68 00 00 45 00G.h.E.
0010	00 5c 13 8f 00 00 31 01 80 54 80 5d a2 53 c0 a81..T.S..
0020	12 65 00 00 ff 85 00 01 00 79 00 00 00 00 00 00y.....
0030	00 00 00 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 00 00 00
0050	00 00 00 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 00 00 00

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.