CS305-2022Spring Lab2 Report

Name：Yitong WANG 11910104@mail.sustech.edu.cn

Student ID：11910104

Lab Time：Thursday 10:20 a.m. to 12:10 p.m.

Lab Teacher：Qing WANG wangq9@mail.sustech.edu.cn

Lab SA:

- Siyu LIU 11912935@mail.sustech.edu.cn
- Xingying ZHENG 11912039@mail.sustech.edu.cn

Practice 1: Find Narcissistic Numbers

- **Source Code**

```
def narcissistic(value: int) -> bool:
    length = len(str(value))
    subs = [int(single) ** length for single in str(value)]
    sum3 = sum(subs)
    del subs
    return sum3 == value


def find_narcissistic_number(start: int, end: int) -> list:
    result = []
    for number in range(start, end + 1, 1):
        if narcissistic(number):
            result.append(number)
    return result


print(' '.join([str(i) for i in find_narcissistic_number(1, 1000000)]))
```

This program can display all the narcissistic numbers from 1 to 1,000,000(including).

- **Commands and Screenshots**

Type this in the command line:

```
python3 narcissistic_number.py
```

And this is the screenshot of the python source code.

```
D:\PycharmProjects\CS305\venv\Scripts\python.exe D:/PycharmProjects/CS305/narcissistic_number.py
1 2 3 4 5 6 7 8 9 153 370 371 407 1634 8208 9474 54748 92727 93084 548834

Process finished with exit code 0
```

Practice 2: Wireshark & curl

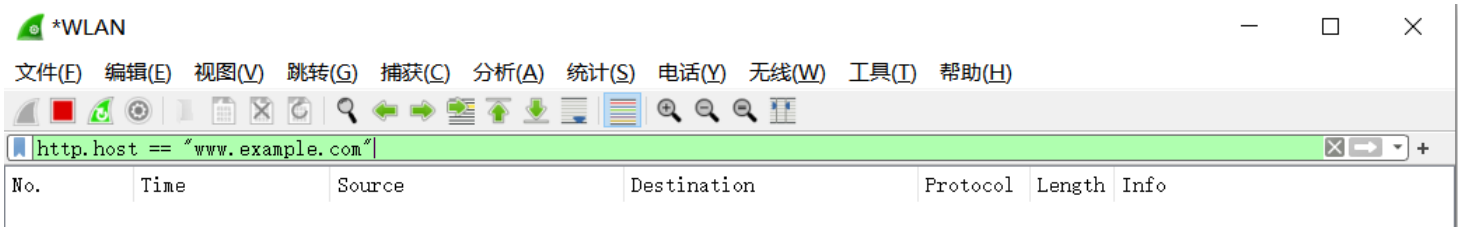
Problem 2-1

Q1

Filter: Capture Filter. Since capture filter can select those packets satisfying the requirements.

Q2

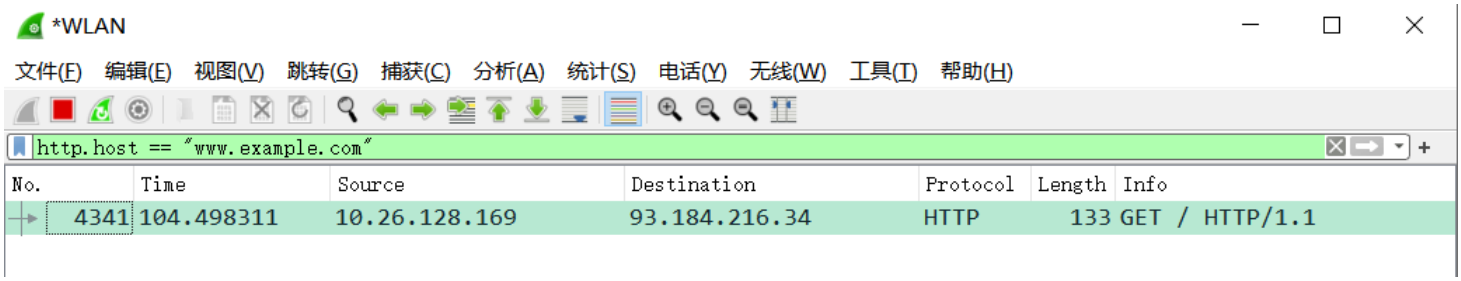
Step 1: Use display filter to find out the ip address of www.example.com. But unfortunately, we cannot find any packets since we haven't built connection with the destination address.



Step 2: Type the following in the command line, so that curl can send request via ipv4.

```
curl --ipv4 www.example.com
```

Then it can be seen that the ip address of www.example.com is 93.184.216.34, and localhost is 10.26.128.169.



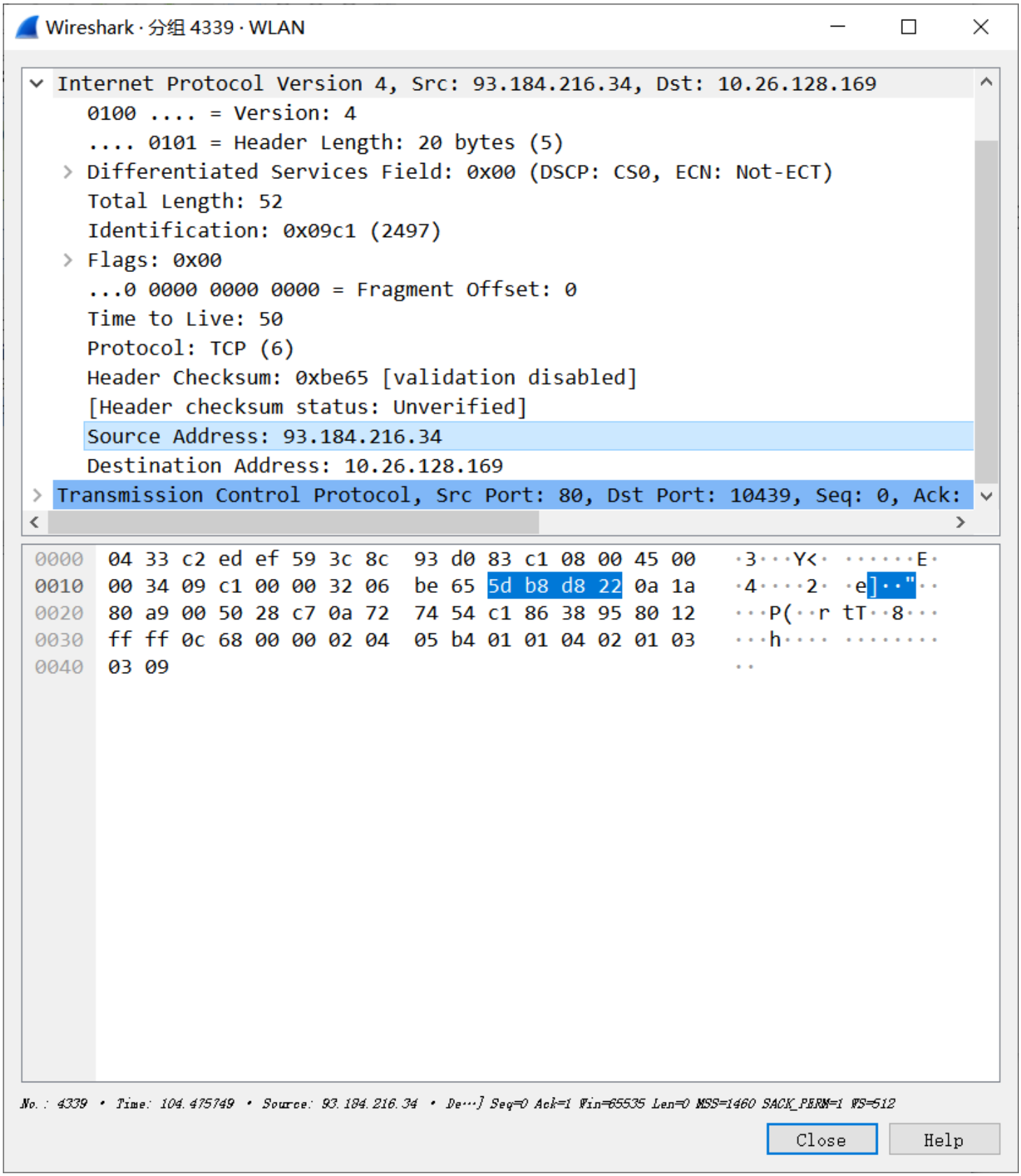
Step 3: Add the new capture filter.

This is the filter requirement:

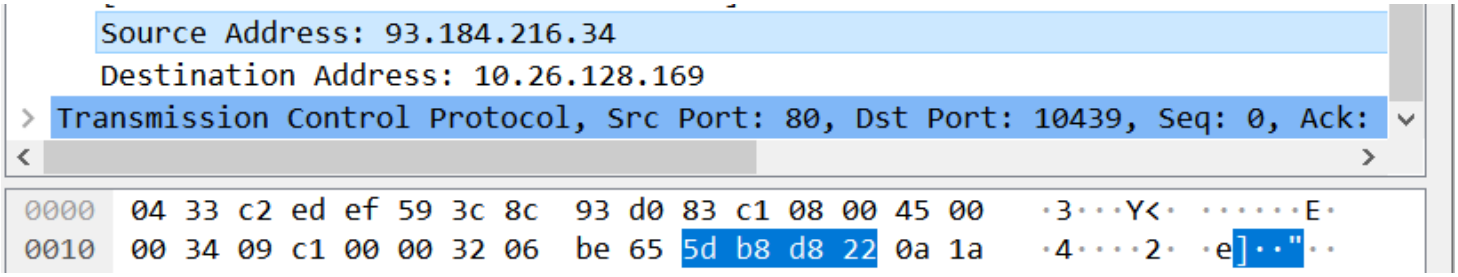
```
src host 93.184.216.34 and dst host 10.26.128.169
```

Step 4: Select a packet we need.

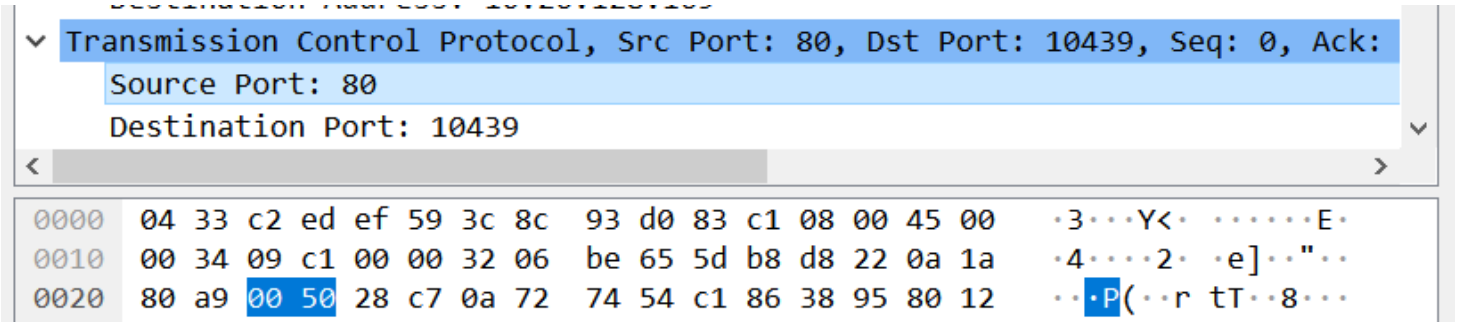
- Packet we select:



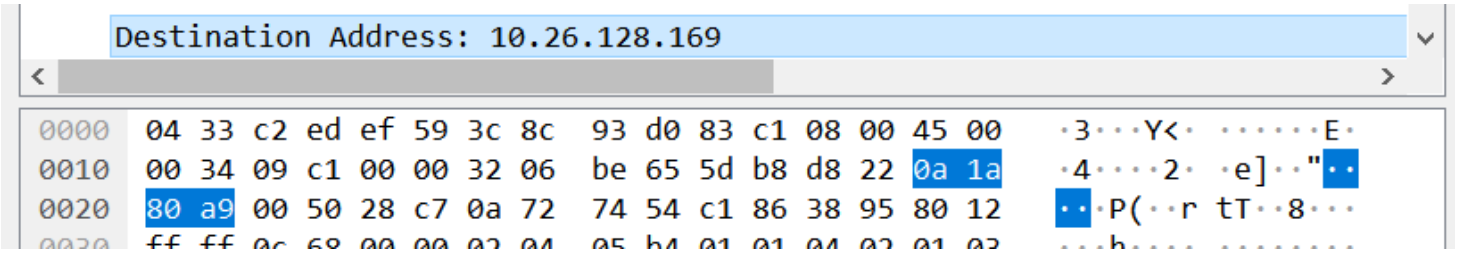
- Source Address



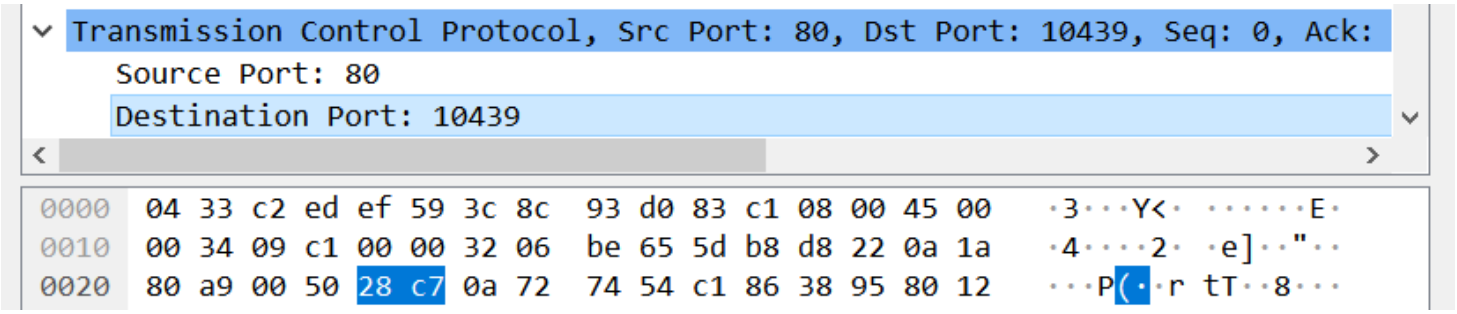
- Source Port



- Destination Address



- Destination Port



We can find these information:

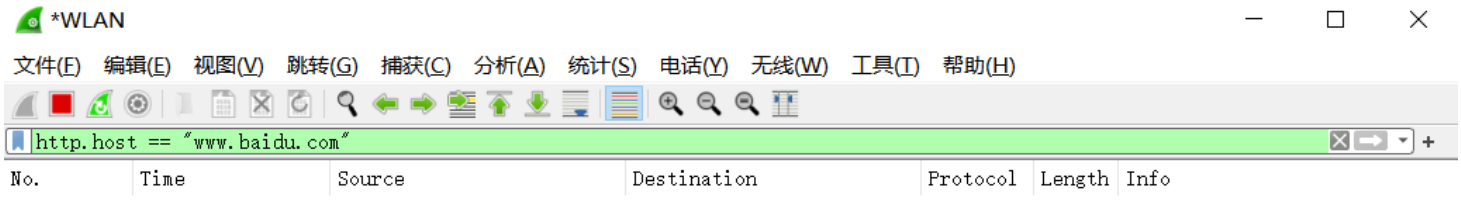
```
Source Address: 93.184.216.34(5d.b8.d8.22 in hexadecimal)
Source Port: 80(0050 in hexadecimal)
Destination Address: 10.26.128.169(0a.1a.80.a9 in hexadecimal)
Destination Port: 10439(28c7 in hexadecimal)
```

Problem 2-2

Q1

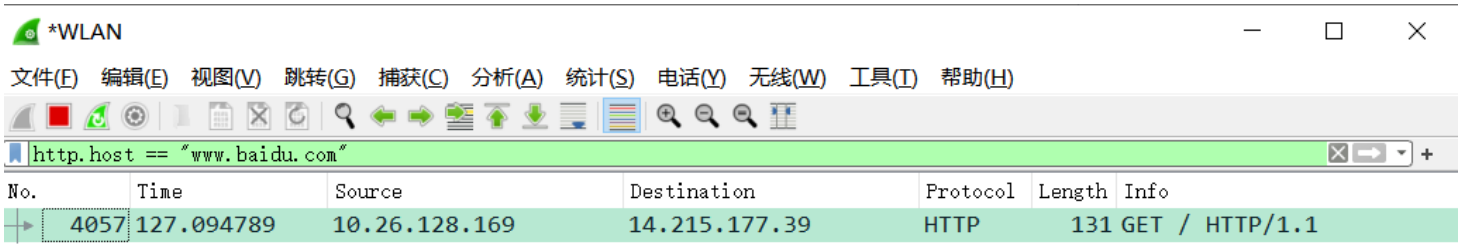
The process of this part is as same as Q2 in Problem 2-1.
So only screenshots and commands will be displayed.

Step 1



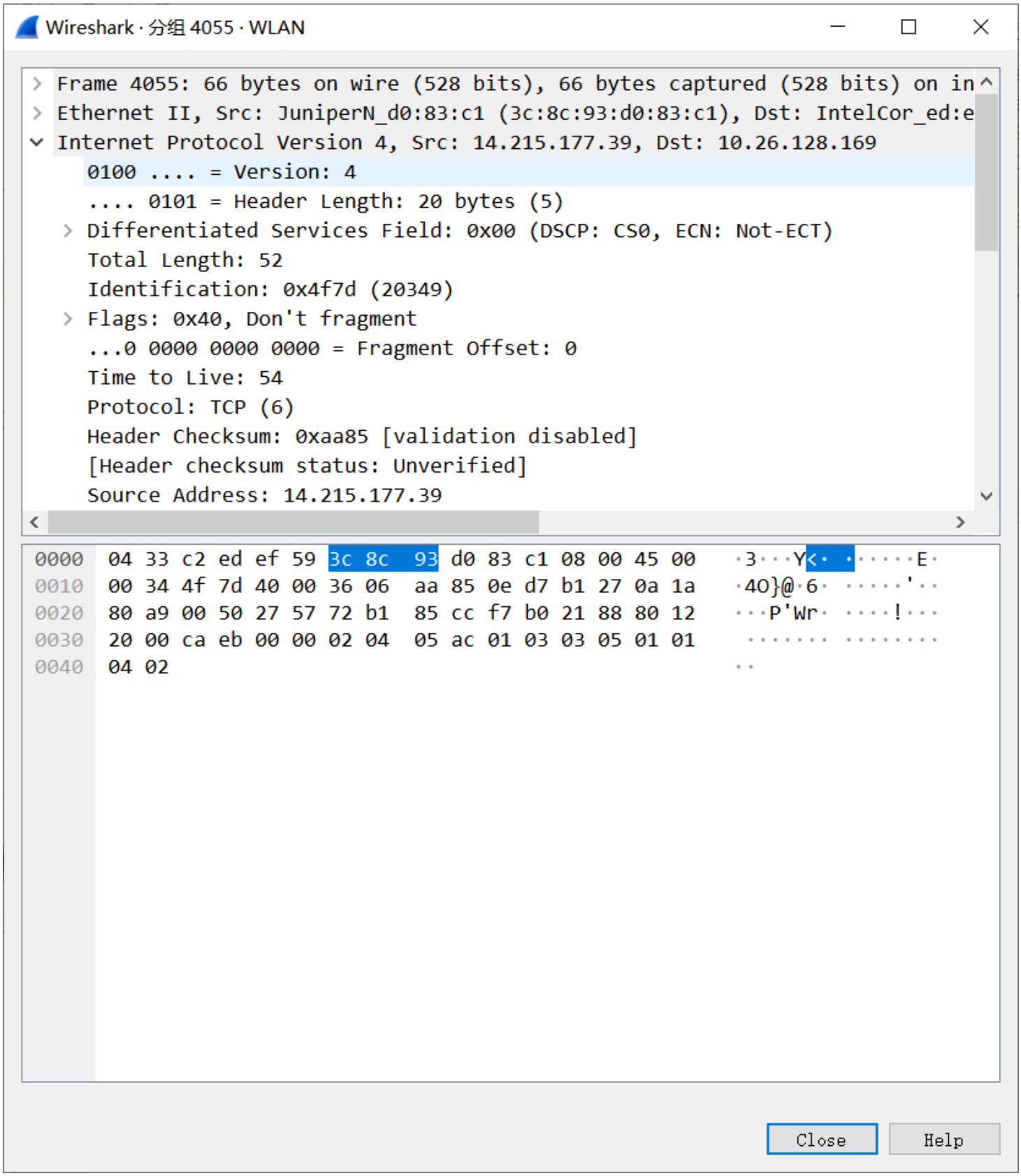
Step 2

```
curl --ipv4 www.baidu.com
```

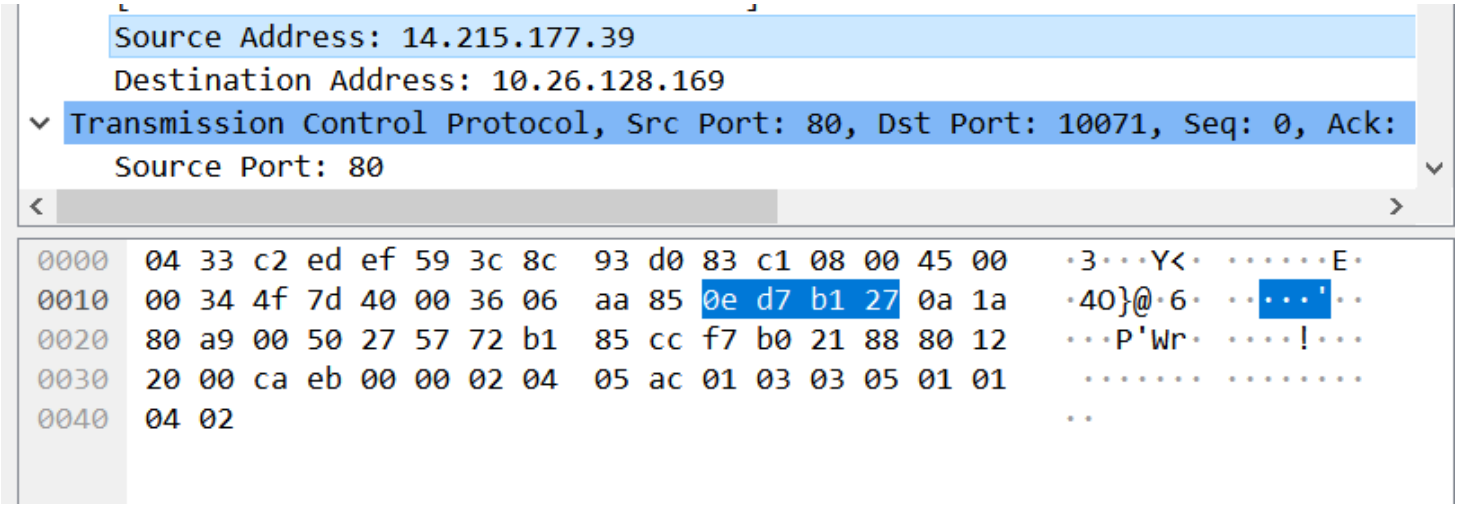


Step 3

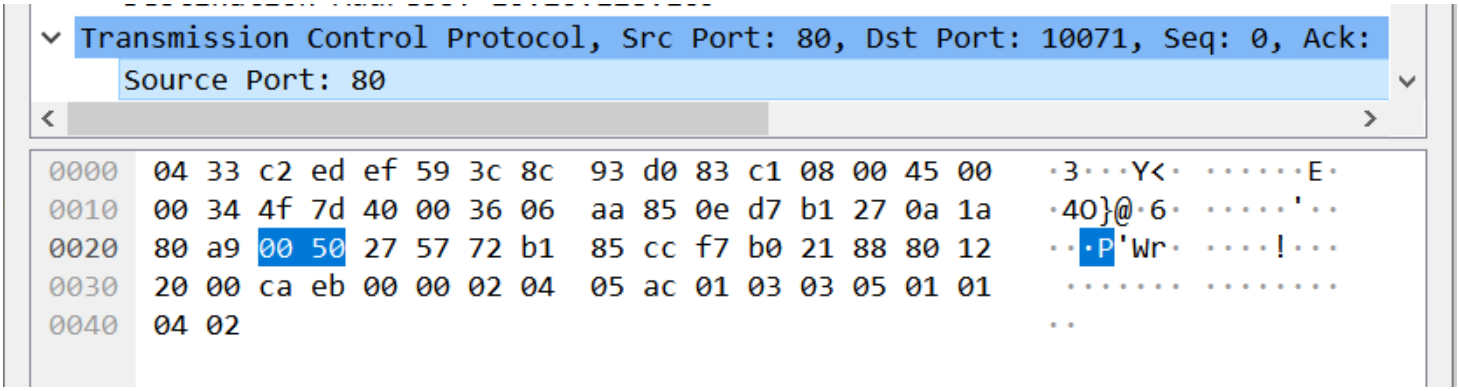
- Packet we select:



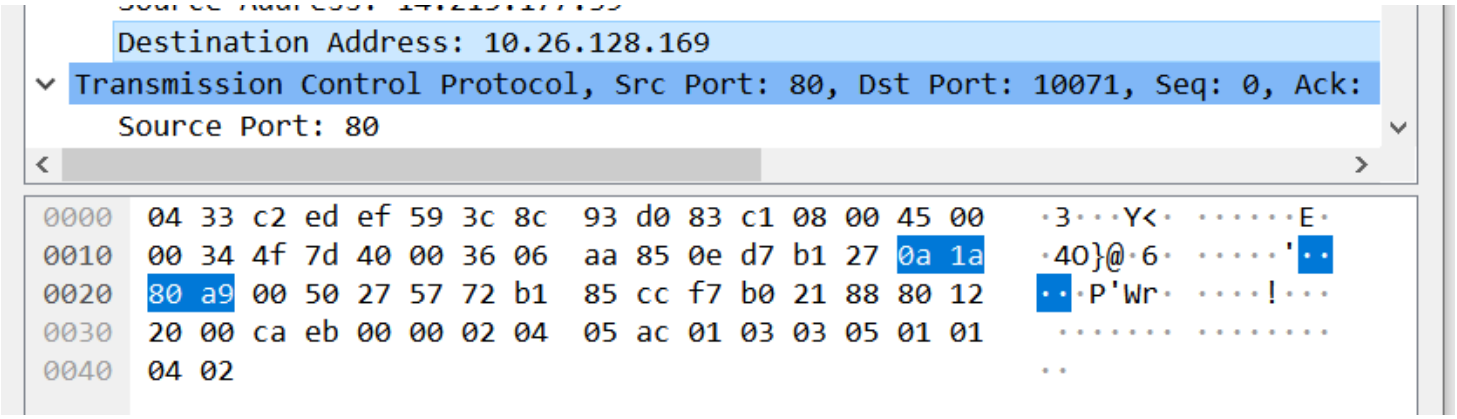
- Source Address:



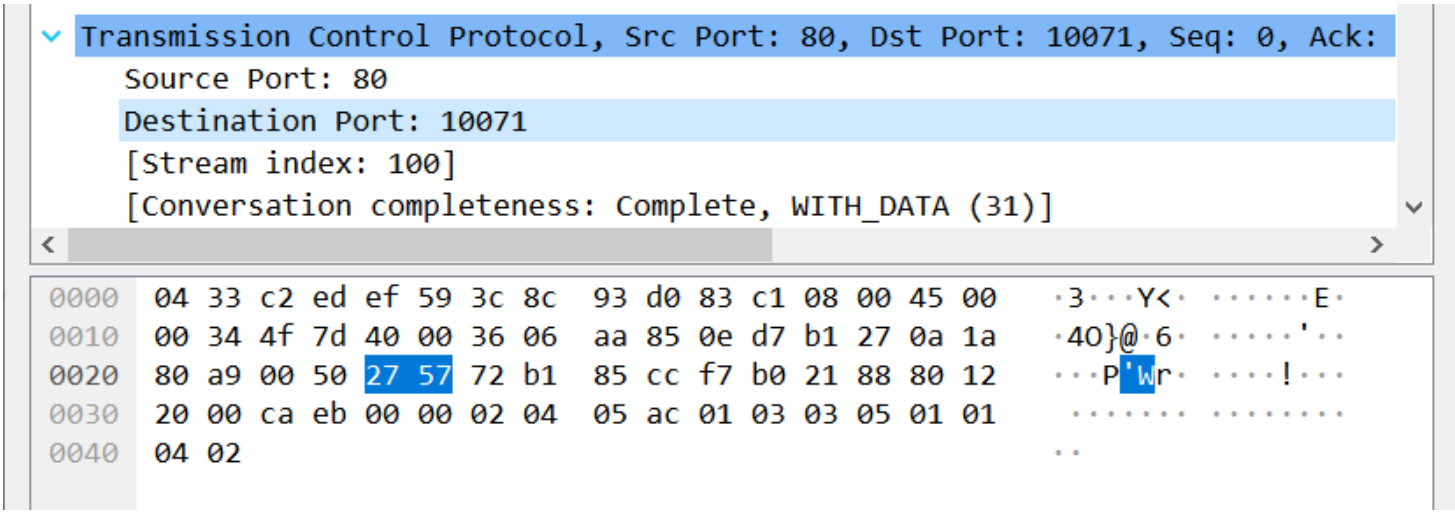
- Source Port:



- Destination Address:



- Destination Port:




```
Source Address: 14.215.177.39(0e.d7.b1.27 in hexadecimal)
Source Port: 80(0050 in hexadecimal)
Destination Address: 10.26.128.169(0a.1a.80.a9 in hexadecimal)
Destination Port: 10071(2757 in hexadecimal)
```

Q2

Comparing the result in Q2 of Problem 2-1 and Q2 of Problem 2-2:

	www.example.com	www.baidu.com
Source Address	93.184.216.34	14.215.177.39
Source Port	80	80
Destination Address	10.126.128.169	10.126.128.169
Destination Port	10439	10071

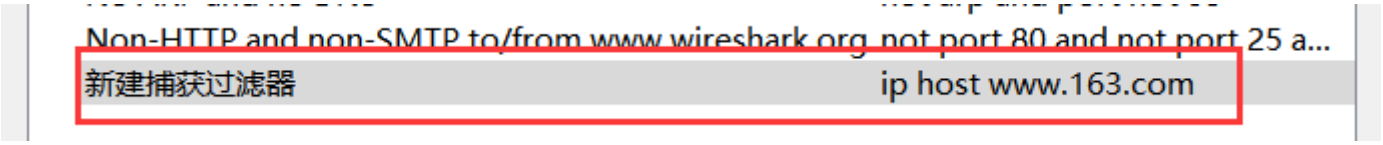
And we can find that the source port and destination address are identical in the two cases.

Practice 3: Wireshark & tracert

Q1

- Step 1: Add capture filter to select those packets whose destination address is www.163.com.

```
ip host www.163.com
```

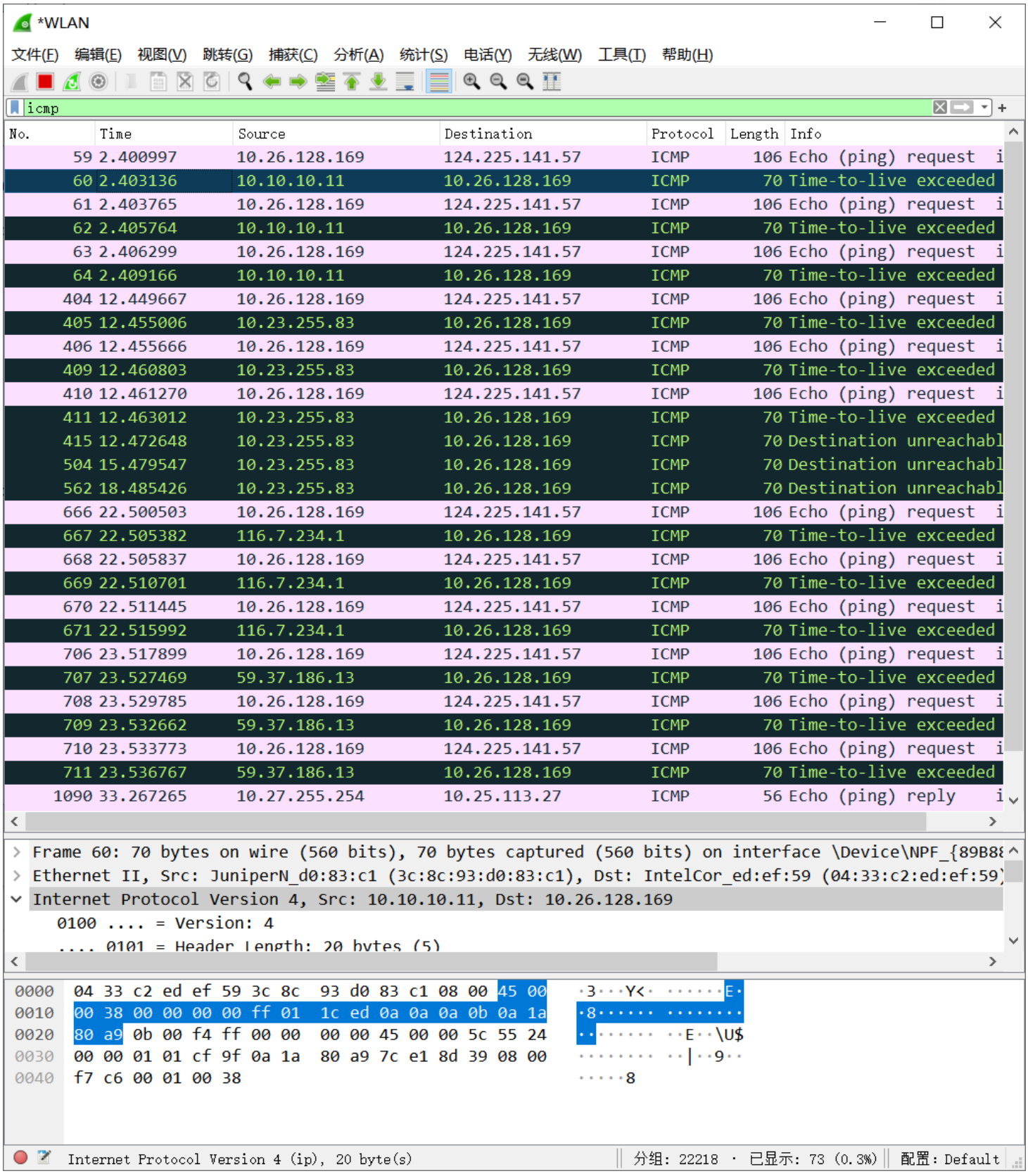


- Step 2: Type the following commands to trace the route:

```
tracert -4 www.163.com
```

```
PS C:\Users\16011\Desktop> tracert -4 www.163.com

通过最多 30 个跃点跟踪
到 z163picipv6.v.bsgslb.cn [124.225.141.57] 的路由:

  1     2 ms     2 ms     2 ms  10.10.10.11
  2     5 ms     5 ms     1 ms  10.23.255.83
  3     5 ms     4 ms     4 ms  group01.its.sustc.edu.cn [116.7.234.1]
  4     9 ms     3 ms     3 ms  13.186.37.59.broad.dg.gd.dynamic.163data.com.cn [59.37.186.13]
  5     3 ms     2 ms     3 ms  117.176.37.59.broad.dg.gd.dynamic.163data.com.cn [59.37.176.117]
  6     3 ms     2 ms     4 ms  14.147.127.41
  7    15 ms    18 ms    15 ms  218.77.143.138
  8    29 ms    15 ms    15 ms  218.77.136.94
  9    68 ms    27 ms    24 ms  124.225.180.54
 10     *        *        *     请求超时。
 11    17 ms    14 ms    14 ms  124.225.141.57

跟踪完成。
PS C:\Users\16011\Desktop>
```

And we can find those packets with display filter `icmp`



Reorganize the packet information, group by Info.

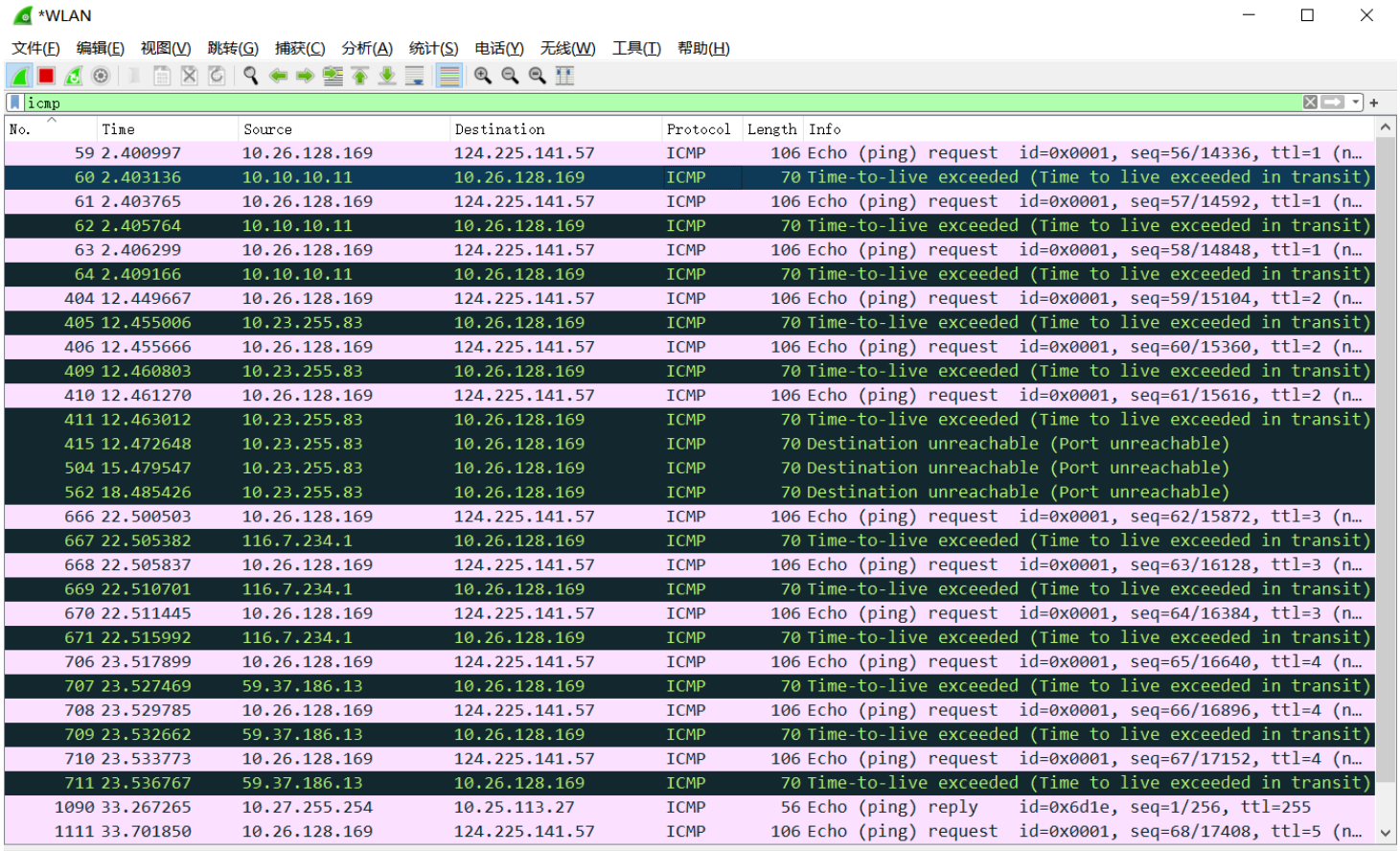
8 echo reply messages

59	2.400997	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=1 (n…
26832	705.840033	10.27.255.254	10.25.107.68	ICMP	118	Echo (ping) reply id=0xa9f9, seq=4/1024, ttl=255
13264	370.943934	10.27.255.254	10.25.6.19	ICMP	118	Echo (ping) reply id=0x9647, seq=3/768, ttl=255
13207	369.796966	10.27.255.254	10.25.6.19	ICMP	118	Echo (ping) reply id=0x9647, seq=2/512, ttl=255
20947	547.573491	10.27.255.254	10.26.129.65	ICMP	1382	Echo (ping) reply id=0x94f2, seq=0/0, ttl=255
1090	33.267265	10.27.255.254	10.25.113.27	ICMP	56	Echo (ping) reply id=0x6d1e, seq=1/256, ttl=255
3175	88.543924	124.225.141.57	10.26.128.169	ICMP	106	Echo (ping) reply id=0x0001, seq=88/22528, ttl=54 (…
3172	88.528622	124.225.141.57	10.26.128.169	ICMP	106	Echo (ping) reply id=0x0001, seq=87/22272, ttl=54 (…
3170	88.512264	124.225.141.57	10.26.128.169	ICMP	106	Echo (ping) reply id=0x0001, seq=86/22016, ttl=54 (…
17923	490.756733	10.26.128.169	172.18.1.93	ICMP	428	Destination unreachable (Port unreachable)

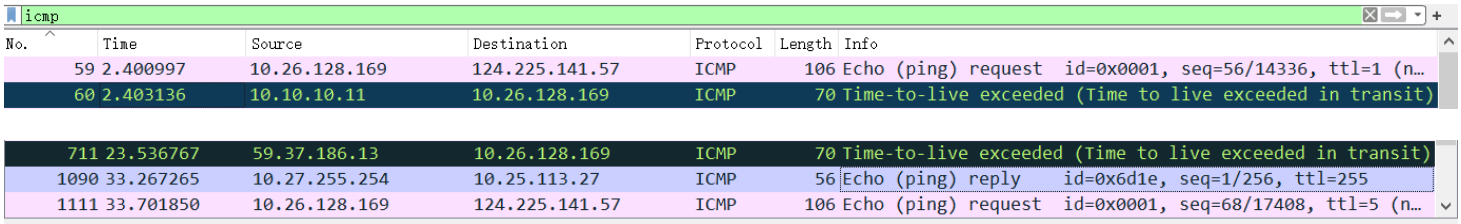
27 time-to-live exceed messages

No.	Time	Source	Destination	Protocol	Length	Info
2303	65.674976	124.225.180.54	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2301	65.650034	124.225.180.54	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
2299	65.621423	124.225.180.54	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1918	55.191114	218.77.136.94	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1915	55.174921	218.77.136.94	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1913	55.156483	218.77.136.94	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1564	44.819068	218.77.143.138	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1562	44.802358	218.77.143.138	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1560	44.783165	218.77.143.138	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1161	34.736009	14.147.127.41	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1159	34.731182	14.147.127.41	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1157	34.727947	14.147.127.41	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1116	33.711965	59.37.176.117	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1114	33.708663	59.37.176.117	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1112	33.705378	59.37.176.117	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
711	23.536767	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
709	23.532662	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
707	23.527469	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
671	22.515992	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
669	22.510701	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
667	22.505382	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
411	12.463012	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
409	12.460803	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
405	12.455006	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
64	2.409166	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
62	2.405764	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
60	2.403136	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
3173	88.529689	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=88/22528, ttl=11 (…

- Step 3: Reorganize the packet information, order by No.

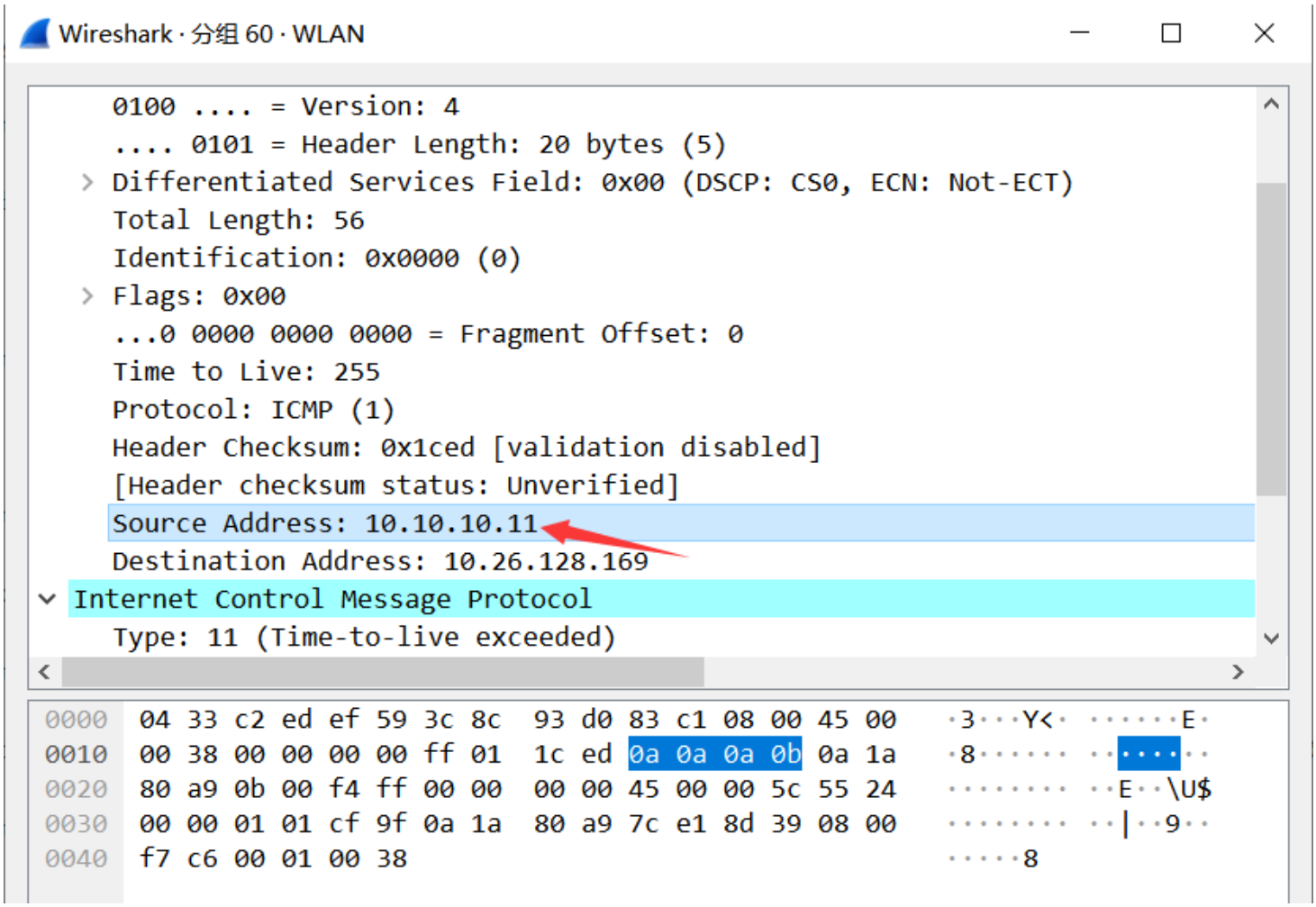


We can find the first received 'time-to-live exceed' message number is 60, and the first received 'echo reply' message number is 1090.

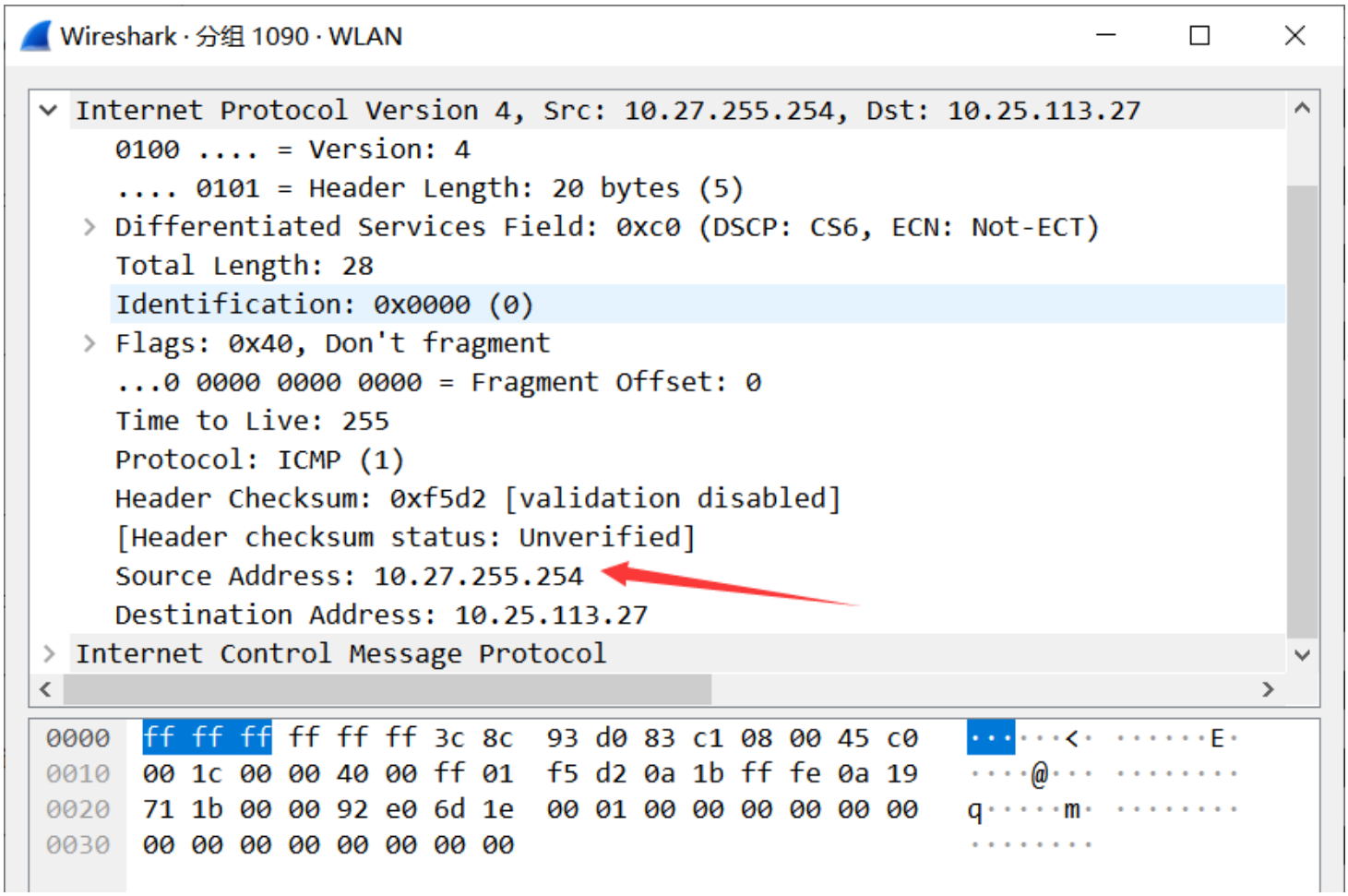


- Step 4: Click and see the details.

First TTL Exceed Source IP Address: 10.10.10.11



First Echo Reply Source IP Address: 10.27.255.254



Q2

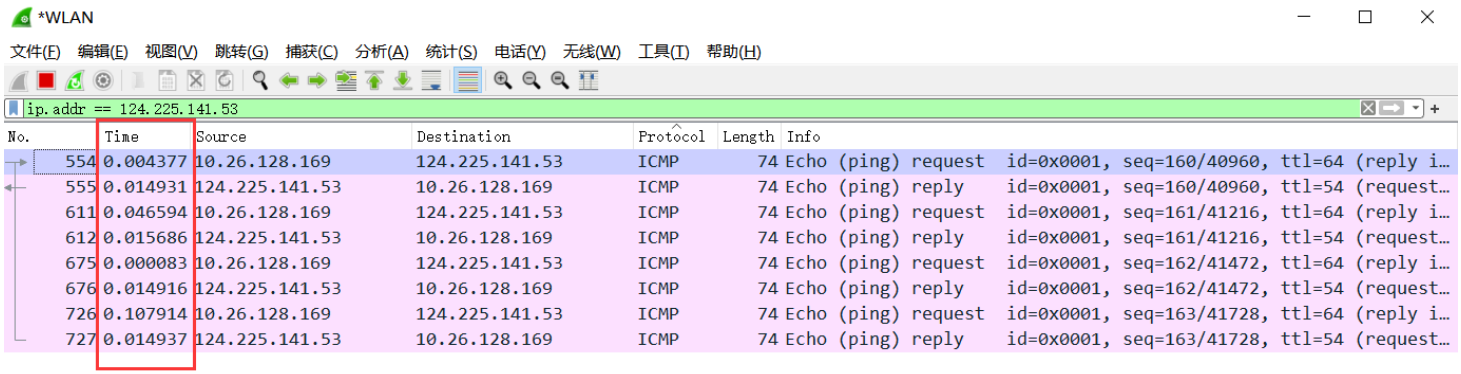
- Step 1: Use the command to calculate RTT.

```
ping -4 www.164.com
```

```
PS C:\Users\16011\Desktop> ping -4 www.163.com

正在 Ping z163picipv6.v.bsgslb.cn [124.225.141.53] 具有 32 字节的数据:
来自 124.225.141.53 的回复: 字节=32 时间=13ms TTL=54
来自 124.225.141.53 的回复: 字节=32 时间=13ms TTL=54
来自 124.225.141.53 的回复: 字节=32 时间=14ms TTL=54
来自 124.225.141.53 的回复: 字节=32 时间=14ms TTL=54

124.225.141.53 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 13ms, 最长 = 14ms, 平均 = 13ms
PS C:\Users\16011\Desktop>
```

We can see the RTT value is 13ms.

- Step 2: Use wireshark to find RTT of all selected packets.



The average value is 0.027430 s = 13.430ms.

We find that this result is almost the same as the command line result.

Q3

- Step 1: Type the following command in the command line.

```
tracert -4 www.163.com
```

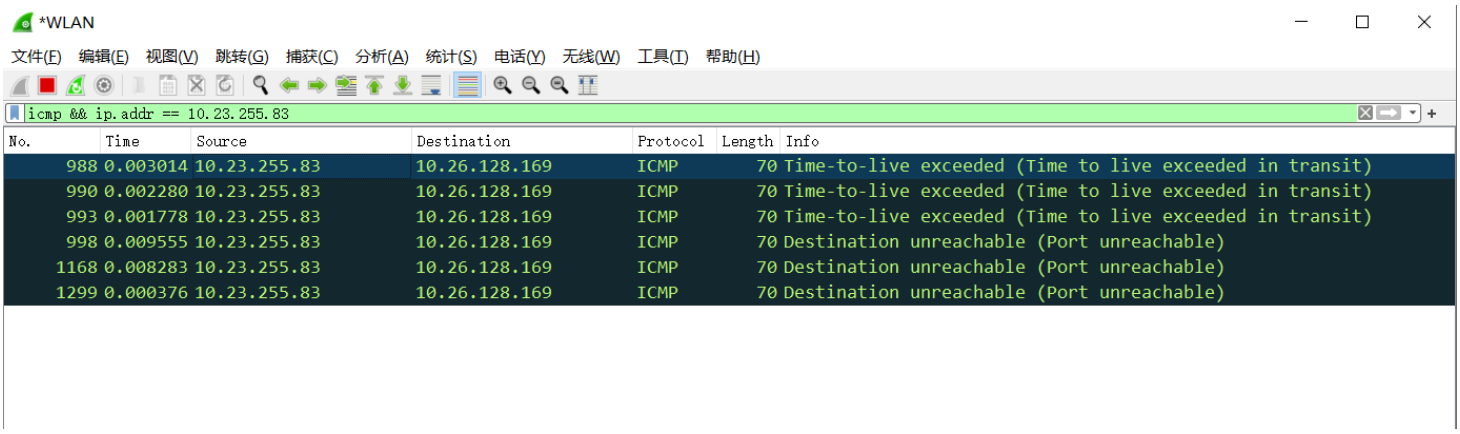
Then we can find the route of accessing www.163.com.

```
PS C:\Users\16011\Desktop> tracert -4 www.163.com

通过最多 30 个跃点跟踪
到 z163picipv6.v.bsgslb.cn [124.225.141.50] 的路由:

  1     2 ms     3 ms     7 ms  10.10.10.11
  2     3 ms     2 ms     2 ms  10.23.255.83
  3    31 ms     8 ms     4 ms  group01.its.sustc.edu.cn [116.7.234.1]
  4     3 ms     2 ms     3 ms  14.147.80.25
  5     *        *        5 ms  117.176.37.59.broad.dg.gd.dynamic.163data.com.cn [59.37.176.117]
  6     *        3 ms     5 ms  202.105.158.69
  7    15 ms    13 ms    14 ms  218.77.143.138
  8     *        *        *     请求超时。
  9    69 ms    46 ms    24 ms  124.225.180.54
 10     *        *        *     请求超时。
 11    14 ms    13 ms    13 ms  124.225.141.50

跟踪完成。
PS C:\Users\16011\Desktop>
```

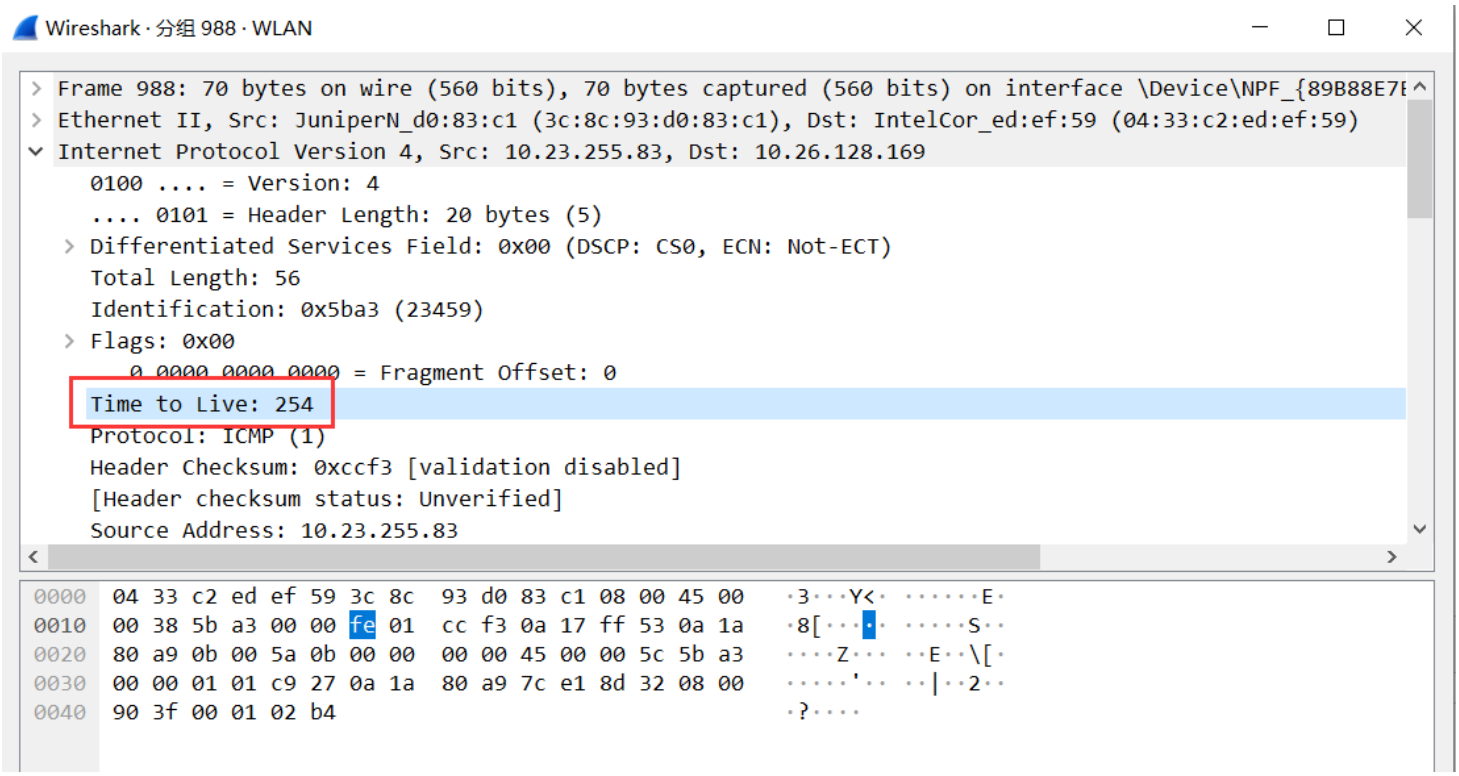
- Step 2: Use Wireshark to find the corresponding packet. (We take the second line with ip address 10.23.255.83 as the example)

Use the following display filter:

```
icmp && ip.addr == 10.23.255.83
```



- Step 3: See the packet TTL information.



We can see the TTL + hop = 254 + 2 = 256, is the constant.

Proof

This sum value is constant, because when the ip hops from one address to another, the TTL value will decrease 1 and hop will increase 1.

If the TTL is 0 after decreasing, then the packet will be processed, or loss.

Therefore, the sum will be an constant value.