

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

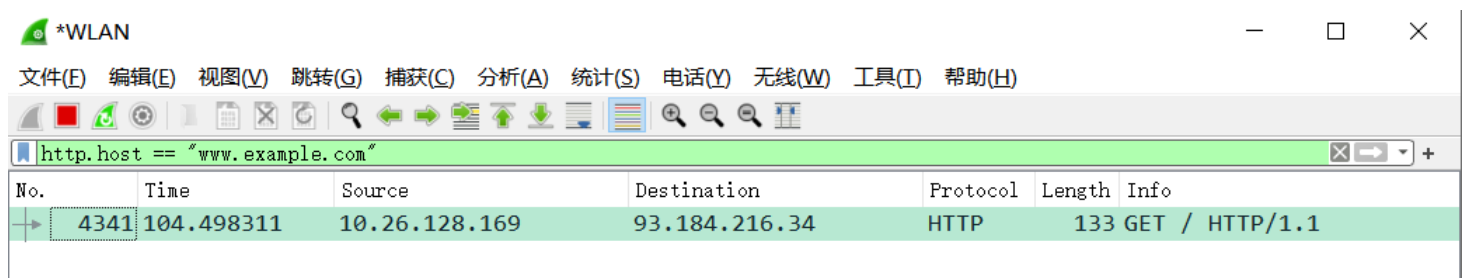
Step 1: Use display filter to find out the ip address of www.example.com. But unfortunately, we cannot find any packets since we haven't built connection with the destination address.



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:

Wireshark · 分组 4339 · WLAN

Internet Protocol Version 4, Src: 93.184.216.34, Dst: 10.26.128.169

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 52
- Identification: 0x09c1 (2497)
- > Flags: 0x00
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 50
- Protocol: TCP (6)
- Header Checksum: 0xbe65 [validation disabled]
[Header checksum status: Unverified]
- Source Address: 93.184.216.34
- Destination Address: 10.26.128.169
- > Transmission Control Protocol, Src Port: 80, Dst Port: 10439, Seq: 0, Ack:

0000 04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00 ·3···Y<· ·····E·
0010 00 34 09 c1 00 00 32 06 be 65 5d b8 d8 22 0a 1a ·4····2· ·e]··"··
0020 80 a9 00 50 28 c7 0a 72 74 54 c1 86 38 95 80 12 ···P(·r tT··8··
0030 ff ff 0c 68 00 00 02 04 05 b4 01 01 04 02 01 03 ···h···· ······
0040 03 09 ..

No.: 4339 · Time: 104.475749 · Source: 93.184.216.34 · De... Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512

Close Help

- Source Address

Source Address: 93.184.216.34
 Destination Address: 10.26.128.169
 > Transmission Control Protocol, Src Port: 80, Dst Port: 10439, Seq: 0, Ack: 1
 < [hex data]

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 09 c1 00 00 32 06 be 65 5d b8 d8 22 0a 1a	·4···2· ·e]··"·

- Source Port

Source Port: 80
 Destination Port: 10439
 < [hex data]

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 09 c1 00 00 32 06 be 65 5d b8 d8 22 0a 1a	·4···2· ·e]··"·
0020	80 a9 00 50 28 c7 0a 72 74 54 c1 86 38 95 80 12	··P(·r tT·8··

- Destination Address

Destination Address: 10.26.128.169
 < [hex data]

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 09 c1 00 00 32 06 be 65 5d b8 d8 22 0a 1a	·4···2· ·e]··"·
0020	80 a9 00 50 28 c7 0a 72 74 54 c1 86 38 95 80 12	··P(·r tT·8··

- Destination Port

Source Port: 80
 Destination Port: 10439
 < [hex data]

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 09 c1 00 00 32 06 be 65 5d b8 d8 22 0a 1a	·4···2· ·e]··"·
0020	80 a9 00 50 28 c7 0a 72 74 54 c1 86 38 95 80 12	··P(·r tT·8··

We can find these information:

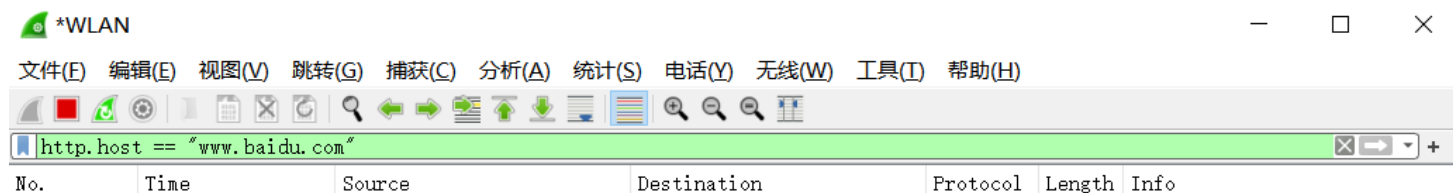
Source Address: 93.184.216.34(5d.b8.d8.22 in hexadecimal)
 Source Port: 80(0050 in hexadecimal)
 Destination Address: 10.26.128.169(0a.1a.80.a9 in hexadecimal)
 Destination Port: 10439(28c7 in hexadecimal)

Problem 2-2

Q1

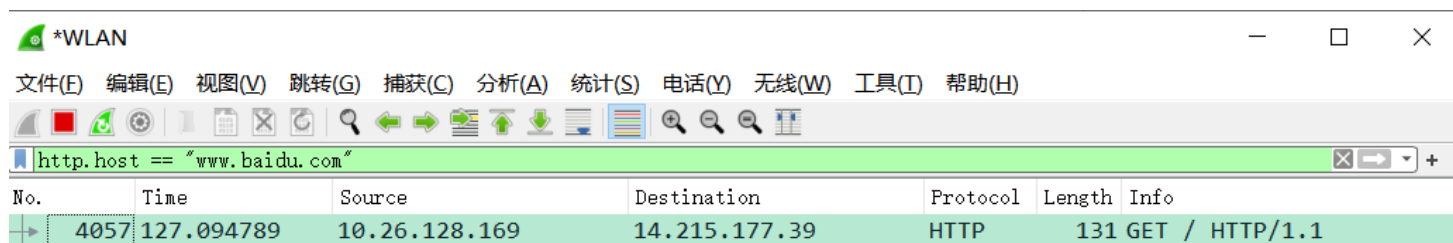
The process of this part is as same as Q2 in Problem 2-1.
So only screenshots and commands will be displayed.

Step 1



Step 2

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



Step 3

- Packet we select:

> Frame 4055: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on in^
 > Ethernet II, Src: JuniperN_d0:83:c1 (3c:8c:93:d0:83:c1), Dst: IntelCor_ed:e
 ▾ Internet Protocol Version 4, Src: 14.215.177.39, Dst: 10.26.128.169

0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 52
 Identification: 0x4f7d (20349)
 > Flags: 0x40, Don't fragment
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 54
 Protocol: TCP (6)
 Header Checksum: 0xaa85 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 14.215.177.39

0000	04 33 c2 ed ef 59	3c 8c 93	d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 4f 7d 40 00 36 06	aa 85 0e d7 b1 27 0a 1a	·40}·@·6· ·····'·	
0020	80 a9 00 50 27 57 72 b1	85 cc f7 b0 21 88 80 12	···P'Wr· ·····!··	
0030	20 00 ca eb 00 00 02 04	05 ac 01 03 03 05 01 01	··············	
0040	04 02		··	

- Source Address:

Source Address: 14.215.177.39

Destination Address: 10.26.128.169

Transmission Control Protocol, Src Port: 80, Dst Port: 10071, Seq: 0, Ack:

Source Port: 80

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 4f 7d 40 00 36 06 aa 85 0e d7 b1 27 0a 1a	·40}·@·6· ·····'·
0020	80 a9 00 50 27 57 72 b1 85 cc f7 b0 21 88 80 12	···P'Wr· ·····!·
0030	20 00 ca eb 00 00 02 04 05 ac 01 03 03 05 01 01	··········
0040	04 02	··

- Source Port:

Transmission Control Protocol, Src Port: 80, Dst Port: 10071, Seq: 0, Ack:

Source Port: 80

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 4f 7d 40 00 36 06 aa 85 0e d7 b1 27 0a 1a	·40}·@·6· ·····'·
0020	80 a9 00 50 27 57 72 b1 85 cc f7 b0 21 88 80 12	···P'Wr· ·····!·
0030	20 00 ca eb 00 00 02 04 05 ac 01 03 03 05 01 01	··········
0040	04 02	··

- Destination Address:

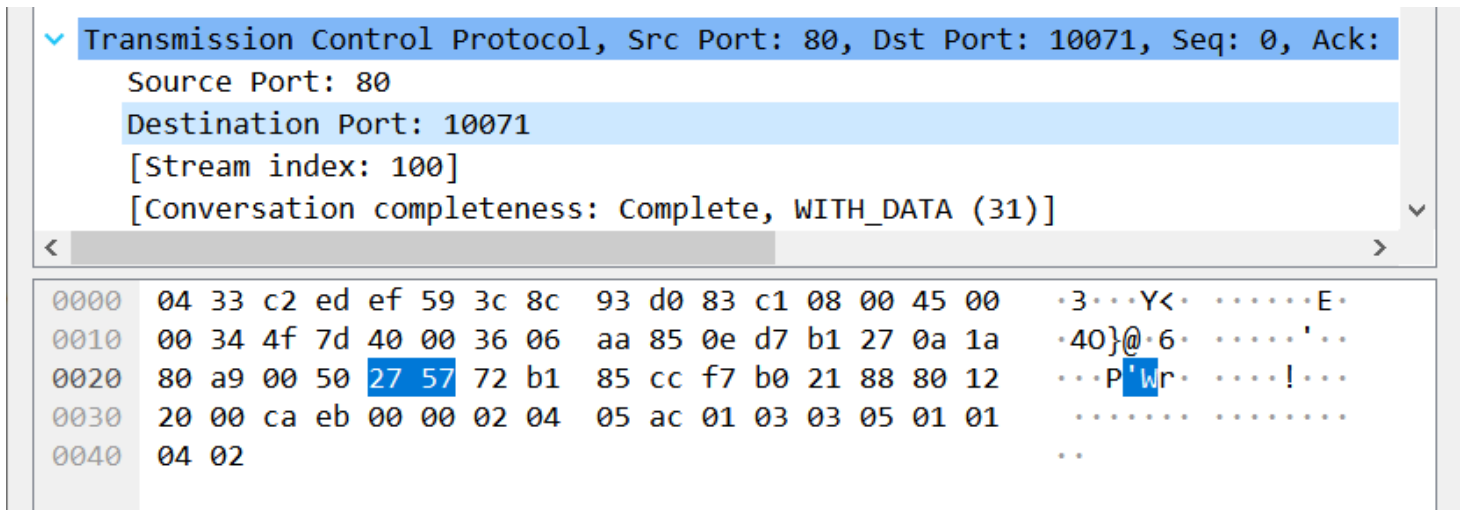
Destination Address: 10.26.128.169

Transmission Control Protocol, Src Port: 80, Dst Port: 10071, Seq: 0, Ack:

Source Port: 80

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ·····E·
0010	00 34 4f 7d 40 00 36 06 aa 85 0e d7 b1 27 0a 1a	·40}·@·6· ·····'·
0020	80 a9 00 50 27 57 72 b1 85 cc f7 b0 21 88 80 12	···P'Wr· ·····!·
0030	20 00 ca eb 00 00 02 04 05 ac 01 03 03 05 01 01	··········
0040	04 02	··

- 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
```


Non-HTTP and non-SMTP to/from www.wireshark.org not port 80 and not port 25 a...

新建捕获过滤器

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

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

icmp

No.	Time	Source	Destination	Protocol	Length	Info
59	2.400997	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
60	2.403136	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded
61	2.403765	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
62	2.405764	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded
63	2.406299	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
64	2.409166	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded
404	12.449667	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
405	12.455006	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded
406	12.455666	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
409	12.460803	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded
410	12.461270	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
411	12.463012	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded
415	12.472648	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachabl
504	15.479547	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachabl
562	18.485426	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachabl
666	22.500503	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
667	22.505382	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded
668	22.505837	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
669	22.510701	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded
670	22.511445	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
671	22.515992	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded
706	23.517899	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
707	23.527469	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded
708	23.529785	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
709	23.532662	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded
710	23.533773	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request i
711	23.536767	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded
1090	33.267265	10.27.255.254	10.25.113.27	ICMP	56	Echo (ping) reply i

> Frame 60: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{89B88}^
 > Ethernet II, Src: JuniperN_d0:83:c1 (3c:8c:93:d0:83:c1), Dst: IntelCor_ed:ef:59 (04:33:c2:ed:ef:59)
 > Internet Protocol Version 4, Src: 10.10.10.11, Dst: 10.26.128.169
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)

```

0000  04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00  .3...Y<.....E.
0010  00 38 00 00 00 00 ff 01 1c ed 0a 0a 0a 0b 0a 1a  .8.....
0020  80 a9 0b 00 f4 ff 00 00 00 00 45 00 00 5c 55 24  ..E..U$
0030  00 00 01 01 cf 9f 0a 1a 80 a9 7c e1 8d 39 08 00  .....|.9..
0040  f7 c6 00 01 00 38                                ....8
  
```

Internet Protocol Version 4 (ip), 20 byte(s) | 分组: 22218 · 已显示: 73 (0.3%) | 配置: Default

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.

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

icmp

No.	Time	Source	Destination	Protocol	Length	Info
59	2.400997	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=1 (n...
60	2.403136	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
61	2.403765	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=57/14592, ttl=1 (n...
62	2.405764	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
63	2.406299	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=58/14848, ttl=1 (n...
64	2.409166	10.10.10.11	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
404	12.449667	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=59/15104, ttl=2 (n...
405	12.455006	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
406	12.455666	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=60/15360, ttl=2 (n...
409	12.460803	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
410	12.461270	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=61/15616, ttl=2 (n...
411	12.463012	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
415	12.472648	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachable (Port unreachable)
504	15.479547	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachable (Port unreachable)
562	18.485426	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachable (Port unreachable)
666	22.500503	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=62/15872, ttl=3 (n...
667	22.505382	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
668	22.505837	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=63/16128, ttl=3 (n...
669	22.510701	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
670	22.511445	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=64/16384, ttl=3 (n...
671	22.515992	116.7.234.1	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
706	23.517899	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=65/16640, ttl=4 (n...
707	23.527469	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
708	23.529785	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=66/16896, ttl=4 (n...
709	23.532662	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
710	23.533773	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=67/17152, ttl=4 (n...
711	23.536767	59.37.186.13	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
1090	33.267265	10.27.255.254	10.25.113.27	ICMP	56	Echo (ping) reply id=0x6d1e, seq=1/256, ttl=255
1111	33.701850	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=5 (n...

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

icmp

No.	Time	Source	Destination	Protocol	Length	Info
59	2.400997	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=56/14336, ttl=1 (n...
60	2.403136	10.10.10.11	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)
1090	33.267265	10.27.255.254	10.25.113.27	ICMP	56	Echo (ping) reply id=0x6d1e, seq=1/256, ttl=255
1111	33.701850	10.26.128.169	124.225.141.57	ICMP	106	Echo (ping) request id=0x0001, seq=68/17408, ttl=5 (n...

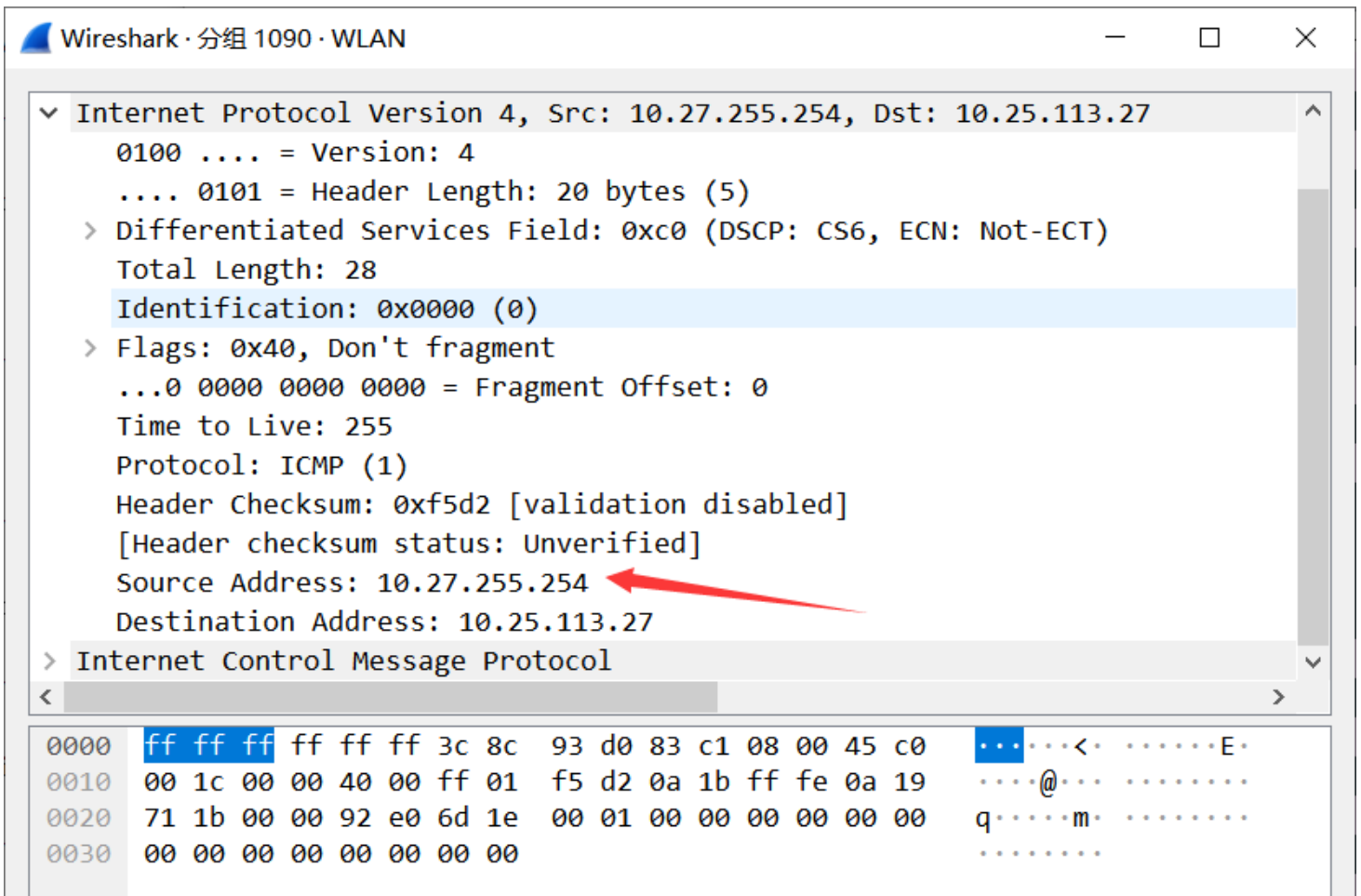
- Step 4: Click and see the details.

First TTL Exceed Source IP Address: 10.10.10.11

0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 56
Identification: 0x0000 (0)
> Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x1ced [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.10.10.11
Destination Address: 10.26.128.169
▼ Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	·3···Y<· ······E·
0010	00 38 00 00 00 00 ff 01 1c ed 0a 0a 0a 0b 0a 1a	·8····· ······
0020	80 a9 0b 00 f4 ff 00 00 00 00 45 00 00 5c 55 24	······· ··E··\U\$
0030	00 00 01 01 cf 9f 0a 1a 80 a9 7c e1 8d 39 08 00	······· ·· ··9··
0040	f7 c6 00 01 00 38	·····8

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.

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

ip.addr == 124.225.141.53

No.	Time	Source	Destination	Protocol	Length	Info
554	0.004377	10.26.128.169	124.225.141.53	ICMP	74	Echo (ping) request id=0x0001, seq=160/40960, ttl=64 (reply i...
555	0.014931	124.225.141.53	10.26.128.169	ICMP	74	Echo (ping) reply id=0x0001, seq=160/40960, ttl=54 (request...
611	0.046594	10.26.128.169	124.225.141.53	ICMP	74	Echo (ping) request id=0x0001, seq=161/41216, ttl=64 (reply i...
612	0.015686	124.225.141.53	10.26.128.169	ICMP	74	Echo (ping) reply id=0x0001, seq=161/41216, ttl=54 (request...
675	0.000083	10.26.128.169	124.225.141.53	ICMP	74	Echo (ping) request id=0x0001, seq=162/41472, ttl=64 (reply i...
676	0.014916	124.225.141.53	10.26.128.169	ICMP	74	Echo (ping) reply id=0x0001, seq=162/41472, ttl=54 (request...
726	0.107914	10.26.128.169	124.225.141.53	ICMP	74	Echo (ping) request id=0x0001, seq=163/41728, ttl=64 (reply i...
727	0.014937	124.225.141.53	10.26.128.169	ICMP	74	Echo (ping) reply id=0x0001, seq=163/41728, ttl=54 (request...

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
```

*WLAN

文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(I) 帮助(H)

icmp && ip.addr == 10.23.255.83

No.	Time	Source	Destination	Protocol	Length	Info
988	0.003014	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
990	0.002280	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
993	0.001778	10.23.255.83	10.26.128.169	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
998	0.009555	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachable (Port unreachable)
1168	0.008283	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachable (Port unreachable)
1299	0.000376	10.23.255.83	10.26.128.169	ICMP	70	Destination unreachable (Port unreachable)

- Step 3: See the packet TTL information.

Wireshark · 分组 988 · WLAN

```

> Frame 988: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{89B88E7E}
> Ethernet II, Src: JuniperN_d0:83:c1 (3c:8c:93:d0:83:c1), Dst: IntelCor_ed:ef:59 (04:33:c2:ed:ef:59)
v Internet Protocol Version 4, Src: 10.23.255.83, Dst: 10.26.128.169
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0x5ba3 (23459)
  > Flags: 0x00
    0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 254
  Protocol: ICMP (1)
  Header Checksum: 0xccf3 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.23.255.83

```

0000	04 33 c2 ed ef 59 3c 8c 93 d0 83 c1 08 00 45 00	.3...Y<.....E.
0010	00 38 5b a3 00 00 fe 01 cc f3 0a 17 ff 53 0a 1a	.8[...S..
0020	80 a9 0b 00 5a 0b 00 00 00 00 45 00 00 5c 5b a3	...Z...E..\[.
0030	00 00 01 01 c9 27 0a 1a 80 a9 7c e1 8d 32 08 002..
0040	90 3f 00 01 02 b4	.?....

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.