CS305-2022Spring Lab11 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

Practice11.1: ICMP

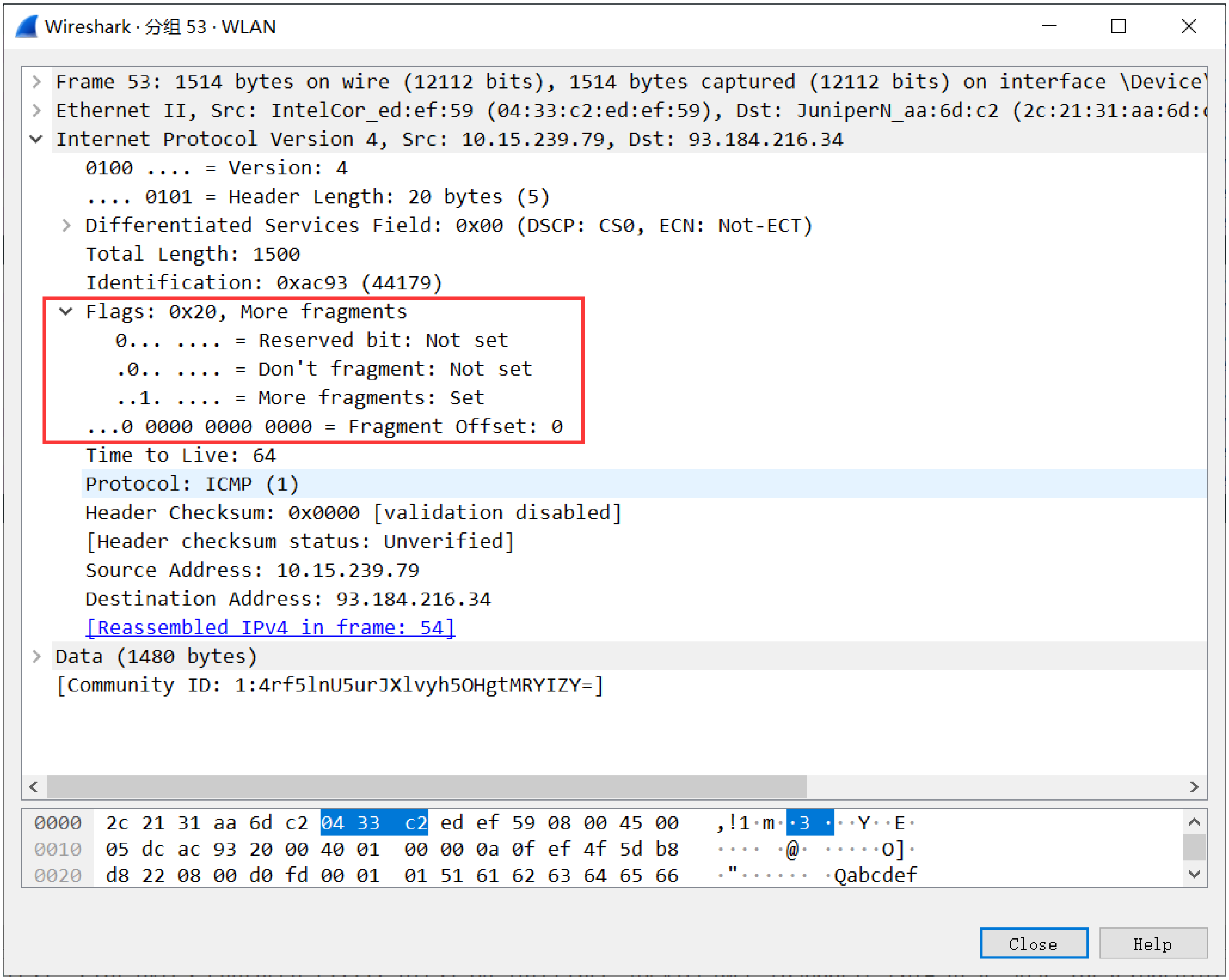
- Q1: How to initiates an ICMP Echo request with 2021B length?

A1: type the following commands in cmd:

```
ping www.example.com -4 -l 2021
```

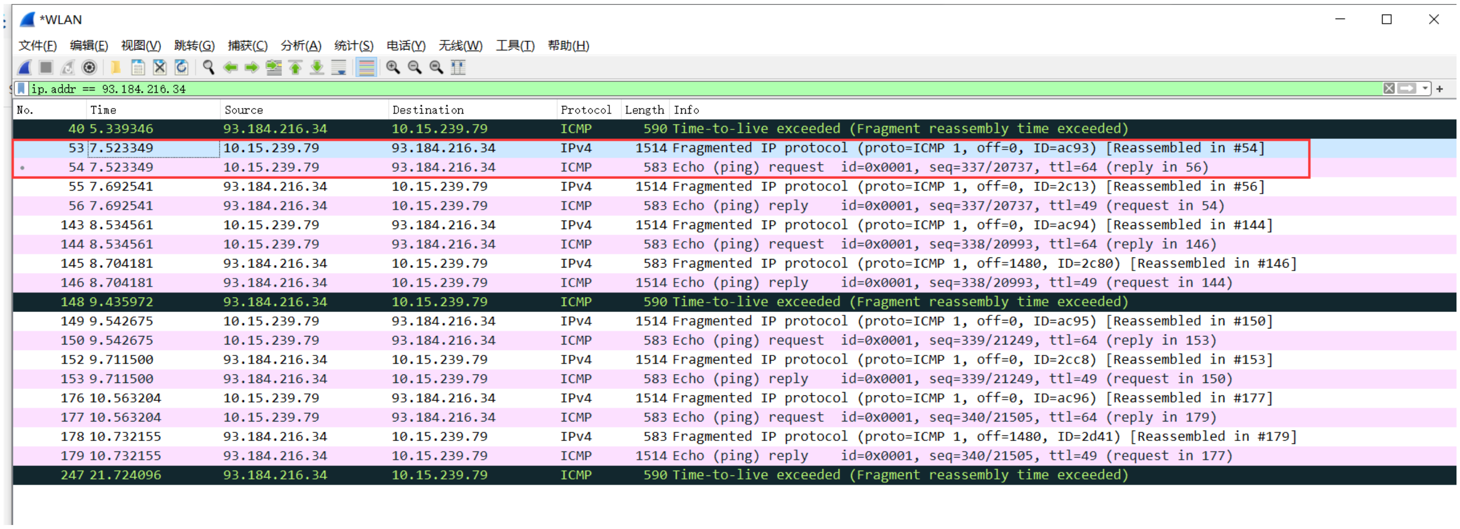
- Q2: Is there any fragmentation on the IP packets, how to find them?

A2: We can see that these packets have fragmentation.

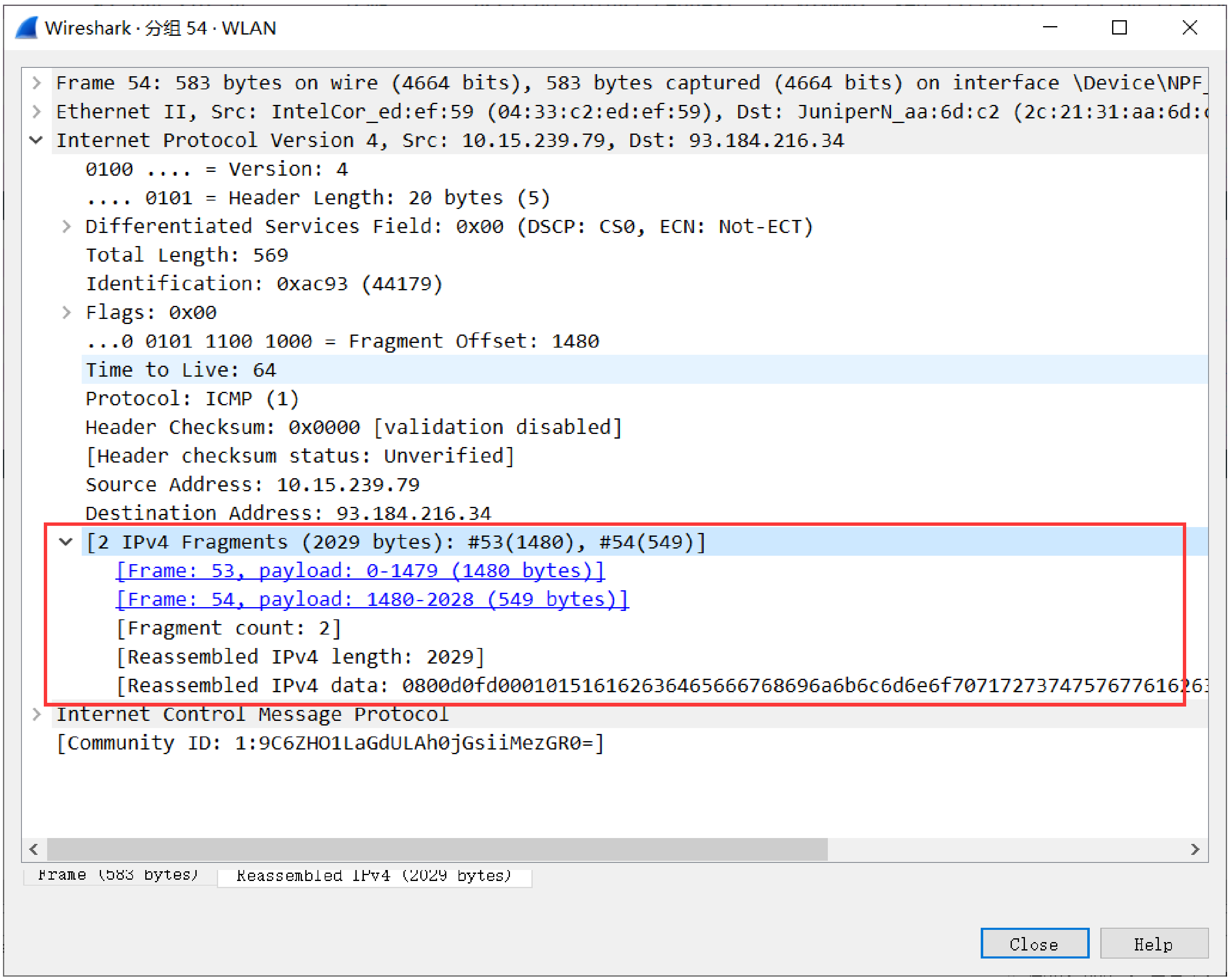


- Q3: How many fragments are the 2021-Byte-length IP packet divided into?

A3: It is divided into two fragments, for each of 2021-Byte-length ip packet.
This is because for two consecutive packets, one is IPv4 and one is ICMP.

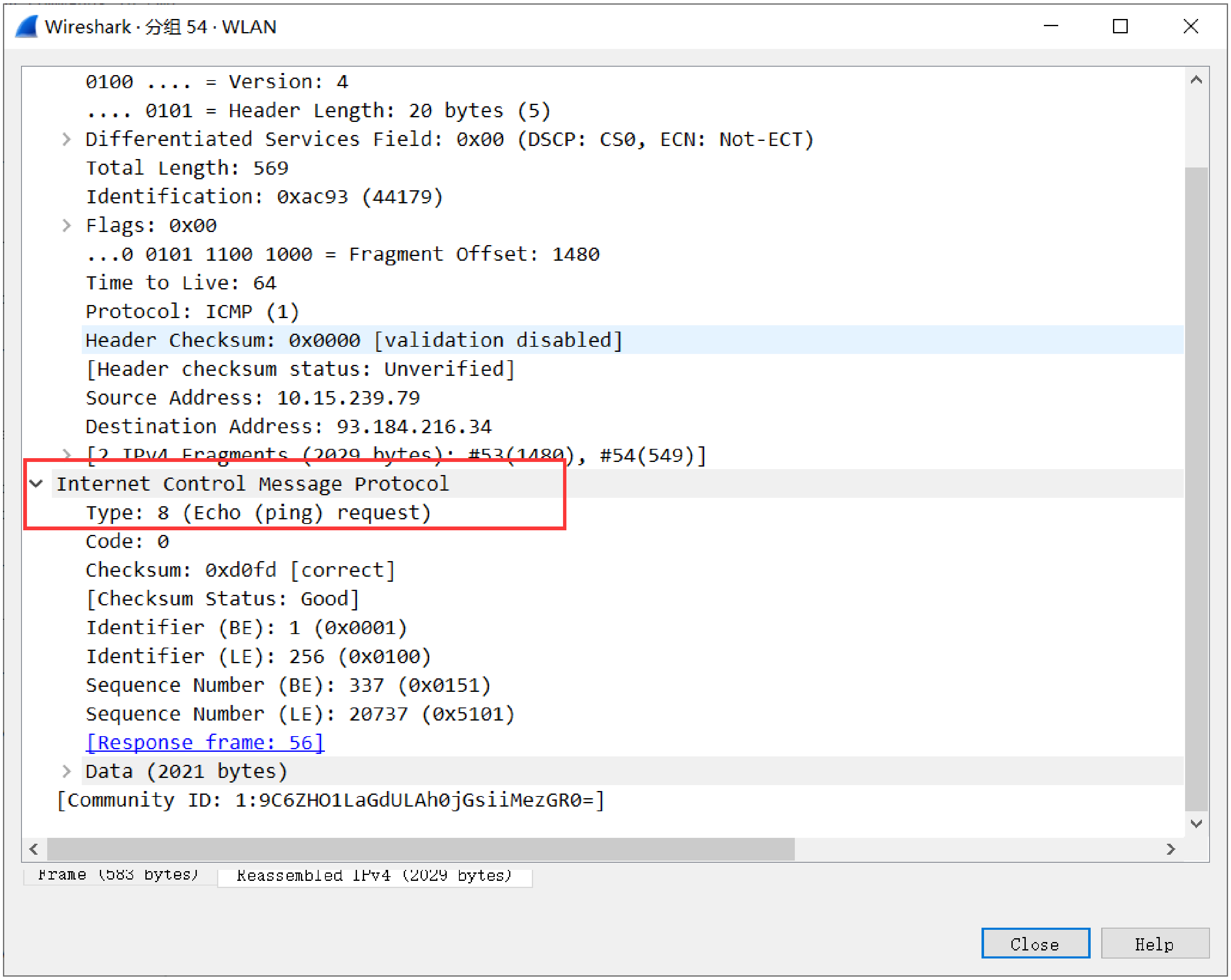


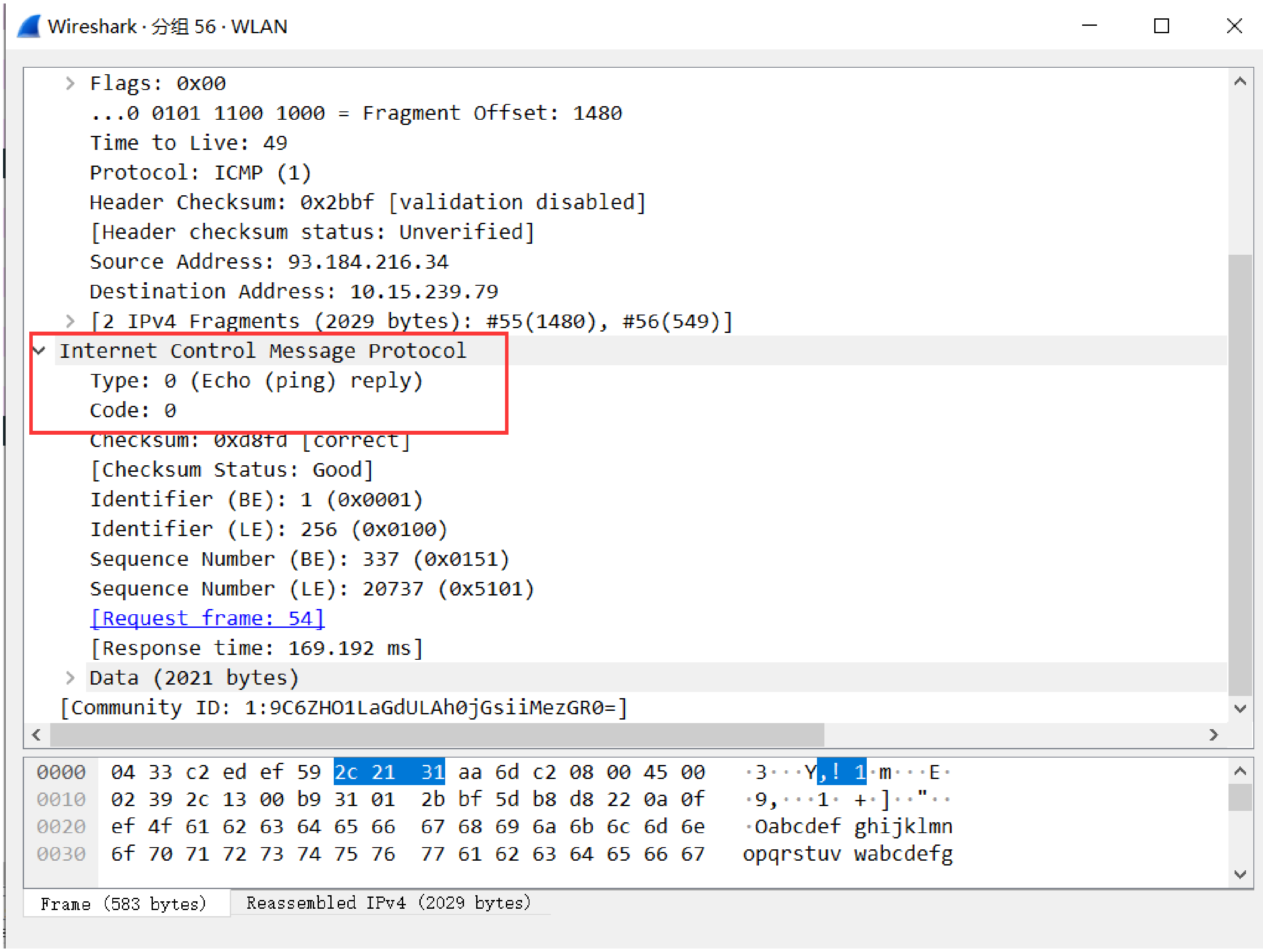
This also supports the idea.



- Q4: How to identify the ICMP Echo request and Echo reply?

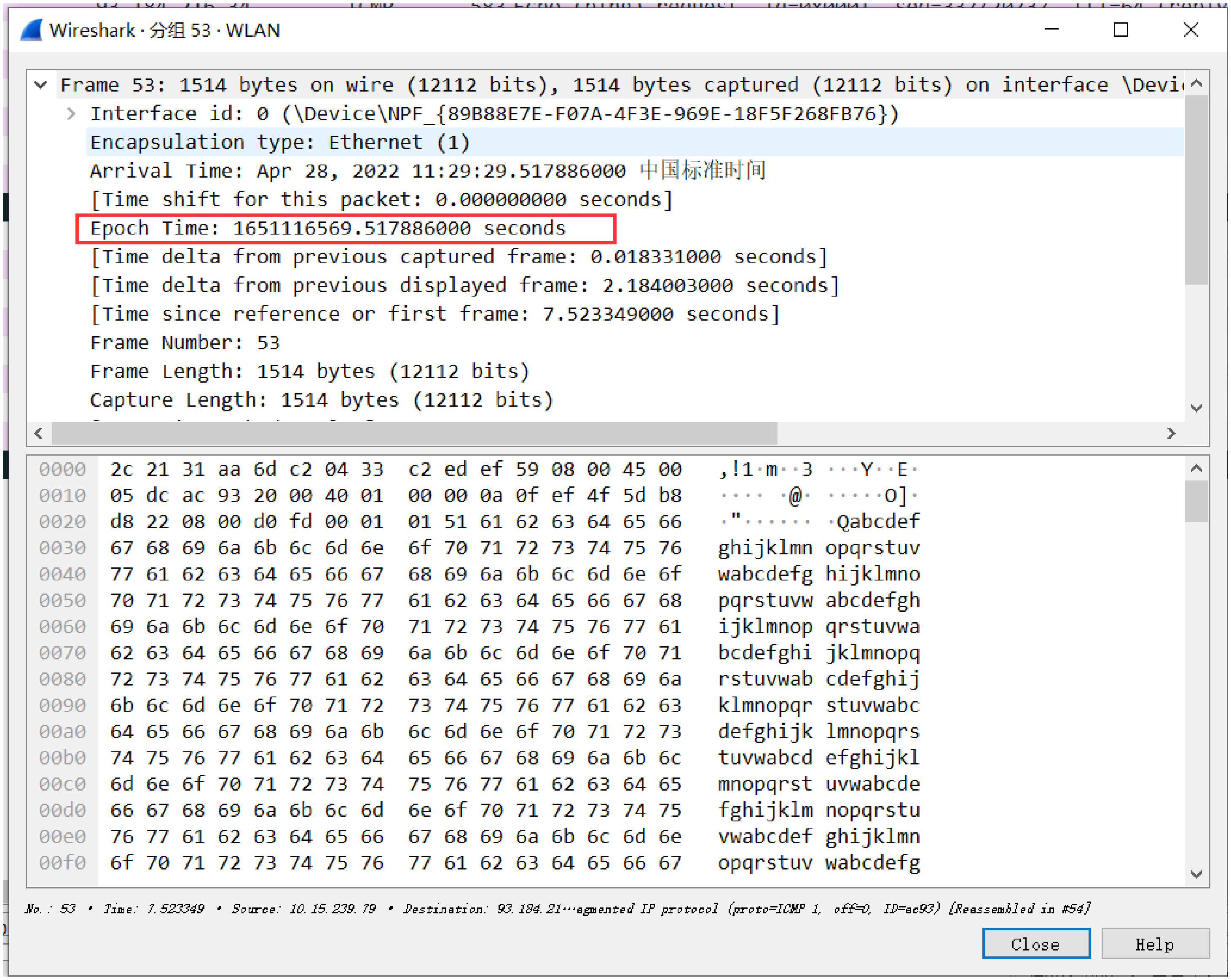
A4: It could be seen in the type information of the packet:


Wireshark · 分组 54 · WLAN
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 569
Identification: 0xac93 (44179)
Flags: 0x00
...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.15.239.79
Destination Address: 93.184.216.34
[2 IPv4 Fragments (2029 bytes): #53(1480), #54(549)]
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xd0fd [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 337 (0x0151)
Sequence Number (LE): 20737 (0x5101)
[Response frame: 56]
Data (2021 bytes)
[Community ID: 1:9C6ZHO1LaGdULAh0jGsiiMezGR0=]
Frame (583 bytes)
Reassembled IPv4 (2029 bytes)
Close
Help



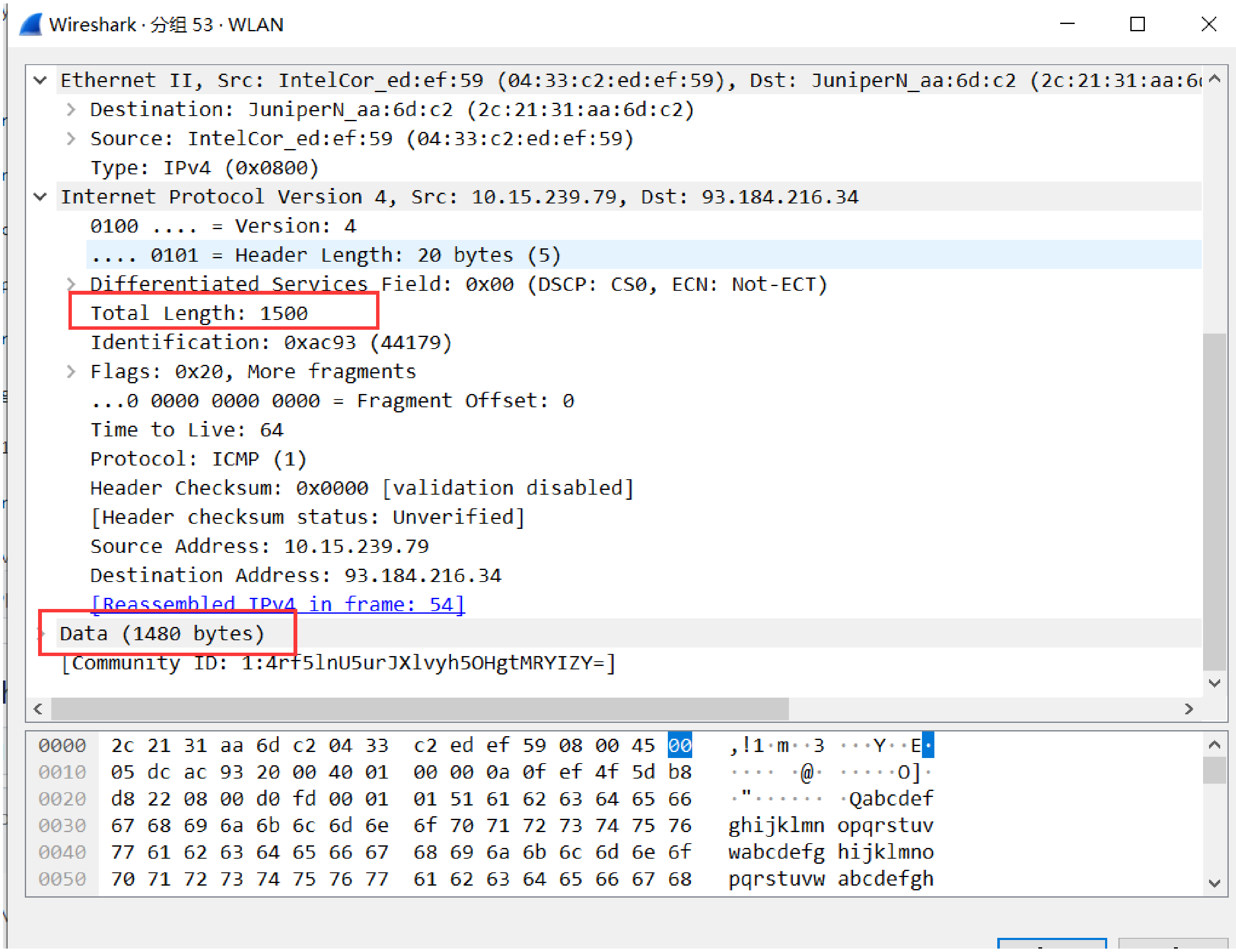
- Q5: For the ICMP Echo request, which fragment is the first one, which is the last ? How to identify them?

A5: In the captured packets, the #53 is the first one, and #177 is the last one. This can be identified by the epoch time.

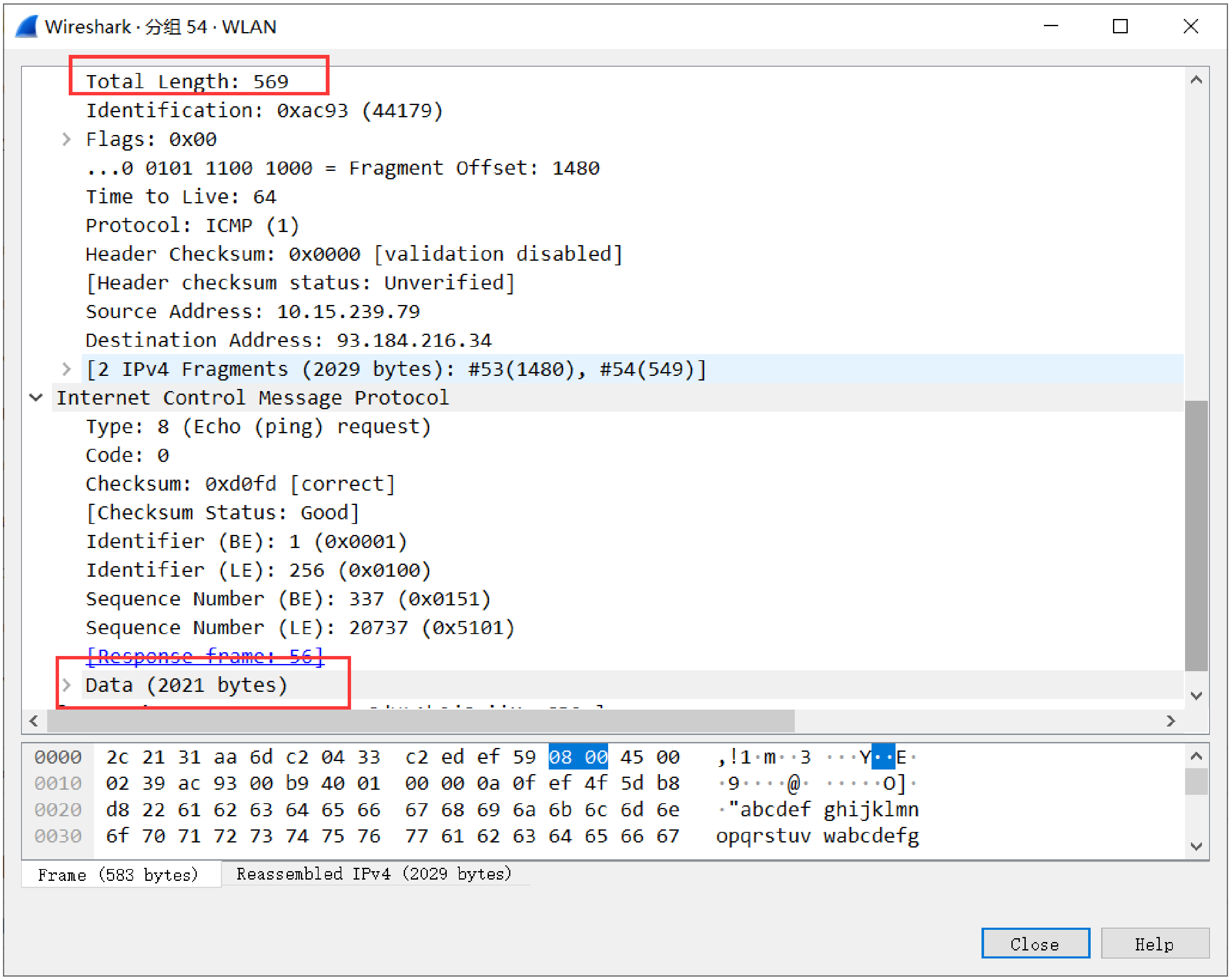


- Q6: What's the length of each IP fragment? Is the sum of each fragment's length equal to the original IP packet?

A6: Take 1 IPv4 and 1 ICMP packet as an example.



The length of the IPv4 fragment is 1500, with 20 header length and 1480 data length.



The length of ICMP fragment is 569, with 20 header length and 2021 data length.

The sum is not equal, 1500 + 569 = 2069 != 2021.

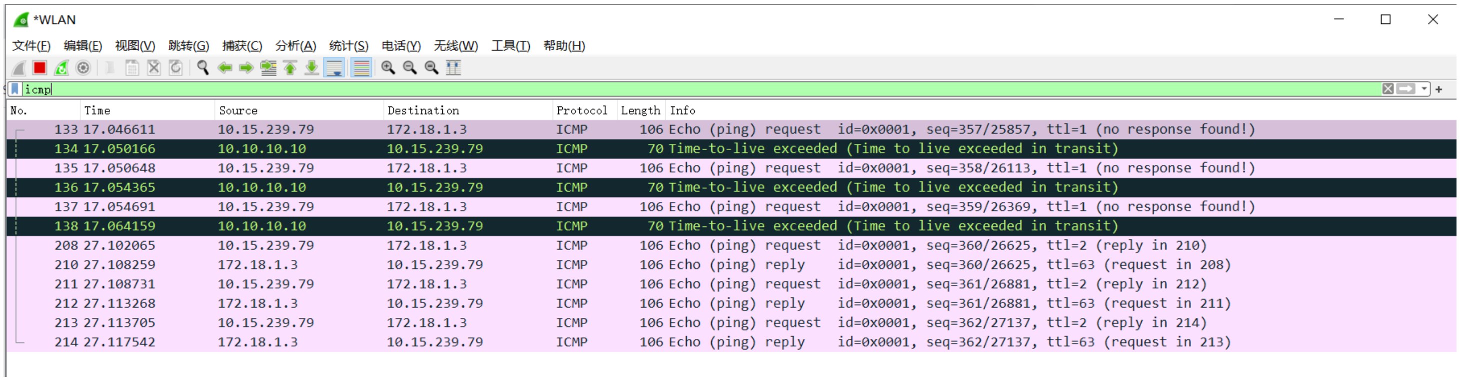
Practice11.2: tracert and ICMP

Commands:

```
tracert -4 www.sustech.edu.cn
```

- Q1: Is there any 'Time-to-live exceeded' ICMP packets?

A1: We can see that there are some 'TTL exceeded' ICMP packets.



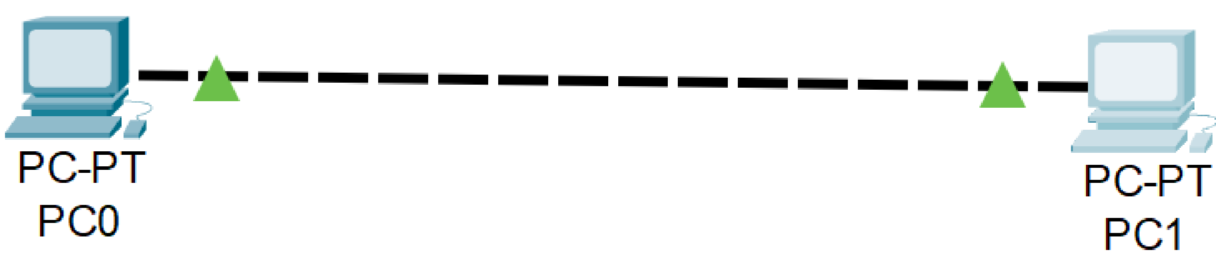
- Q2: What's the difference between these ICMP packets which are invoked by 'tracert' and ICMP echo request/replay packets which are invoked by 'ping'?

A2: Differences:

1. The total length of packets caused by `tracert` is much smaller than those by `ping`. The total length is 56 in `tracert` while 1500 in `ping`.
2. The packet by `ping` will contain a original packet(2021 bytes), while not by `tracert`
3. The TTL is not the same.

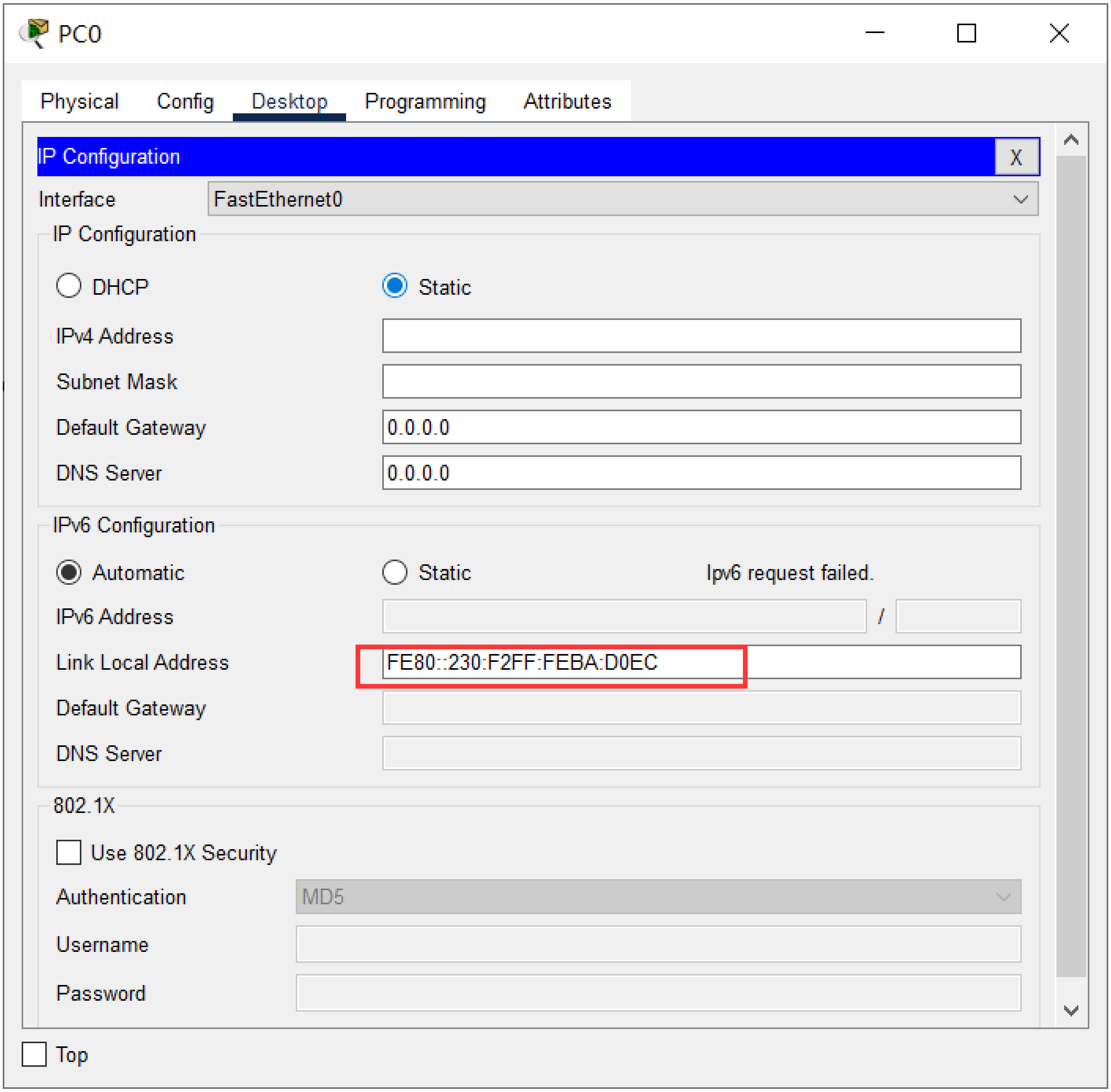
Practice11.3: Packet-tracer and ICMP

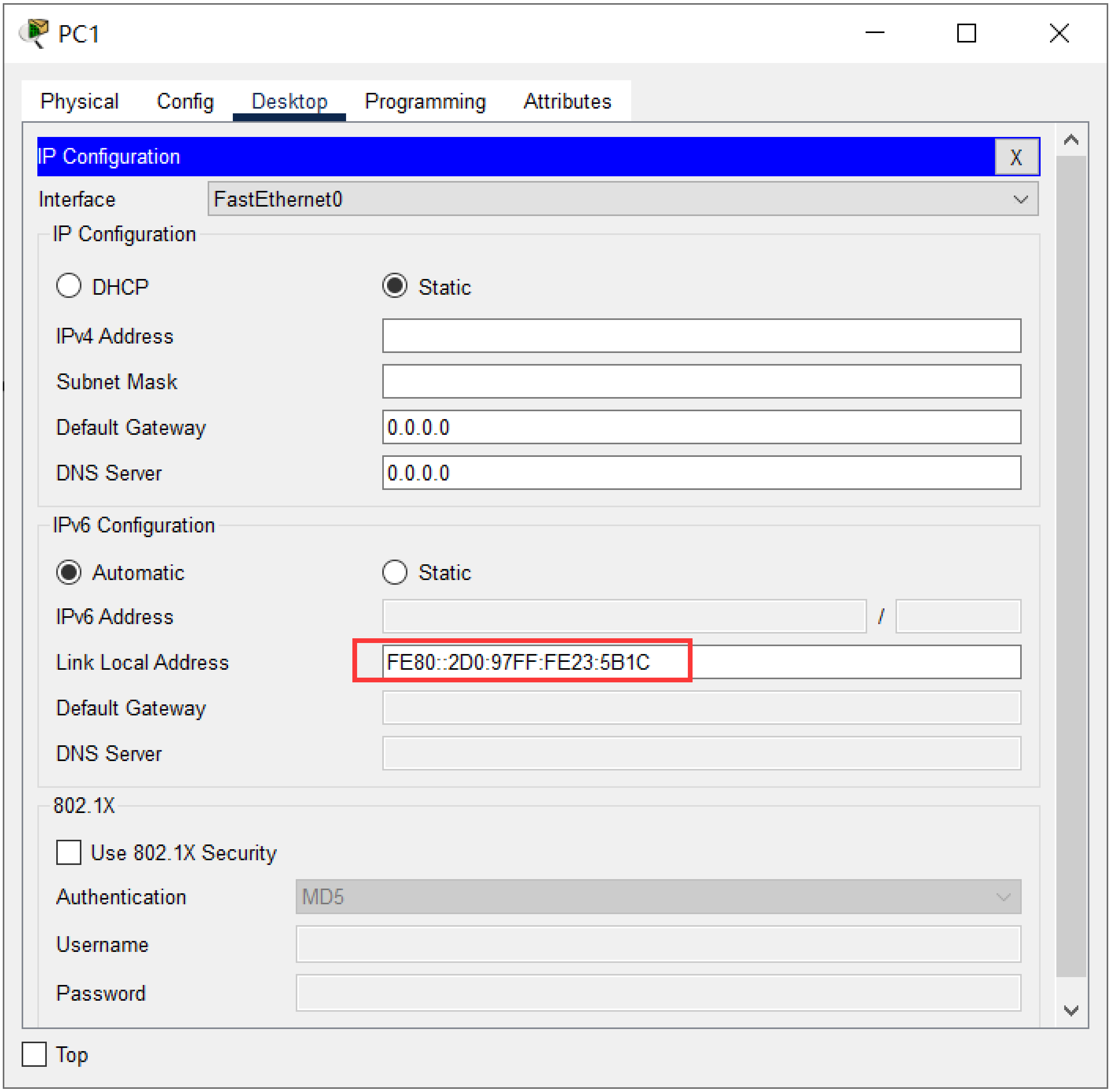
Build connection first:



- Q1: What's link-local unicast IPv6 address of these 2 PCs?

A1: Check the ip configuration of these two PCs.


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
Subnet Mask
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
Ipv6 request failed.
IPv6 Address
/
Link Local Address
FE80::230:F2FF:FEBA:D0EC
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top



We can get the IPv6 address:

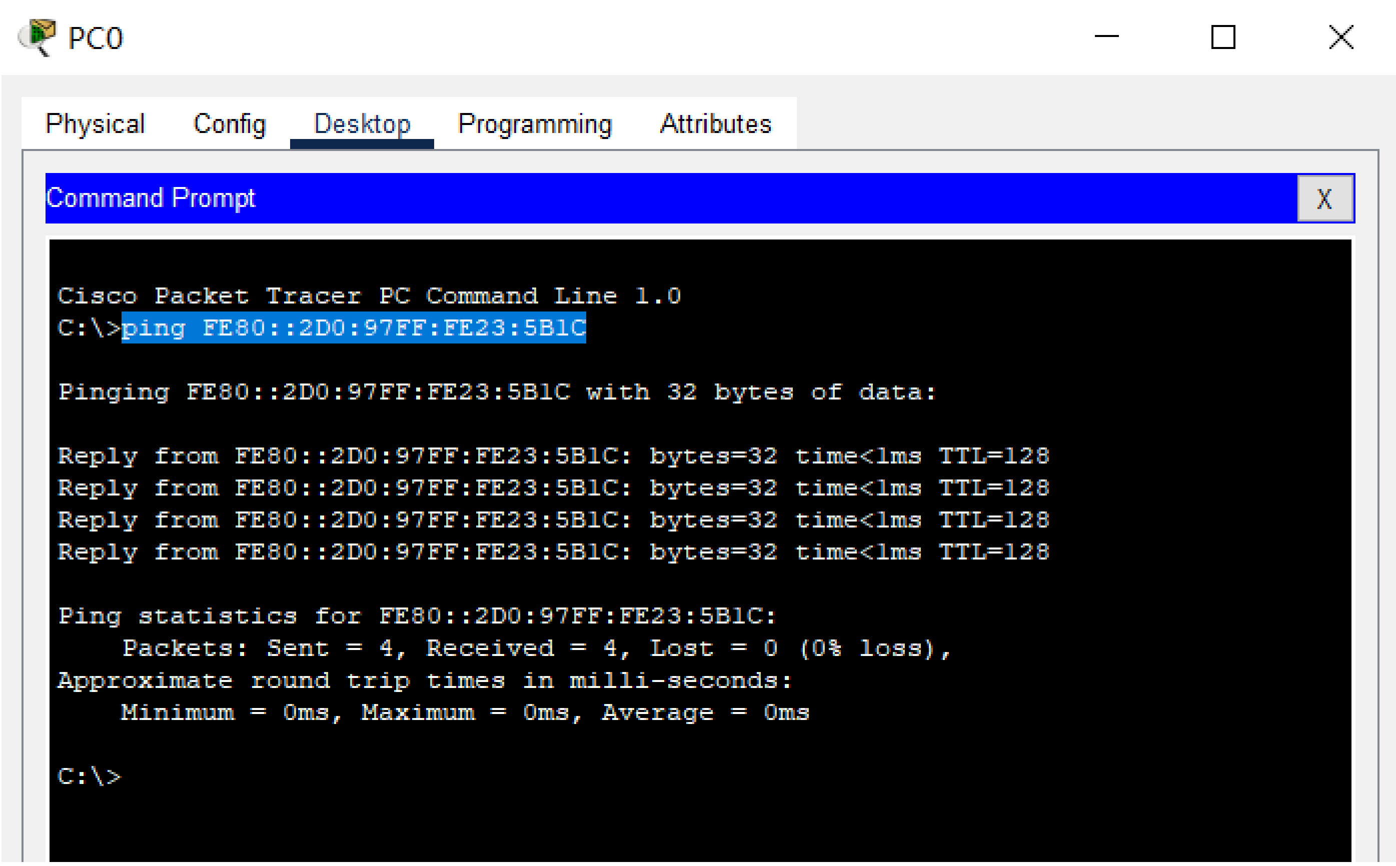
PC0: FE80::230:F2FF:FEBA:D0EC

PC1: FE80::2D0:97FF:FE23:5B1C

- Q2: Initiates an ICMPv6 session on PC0 to PC1, capture the packets

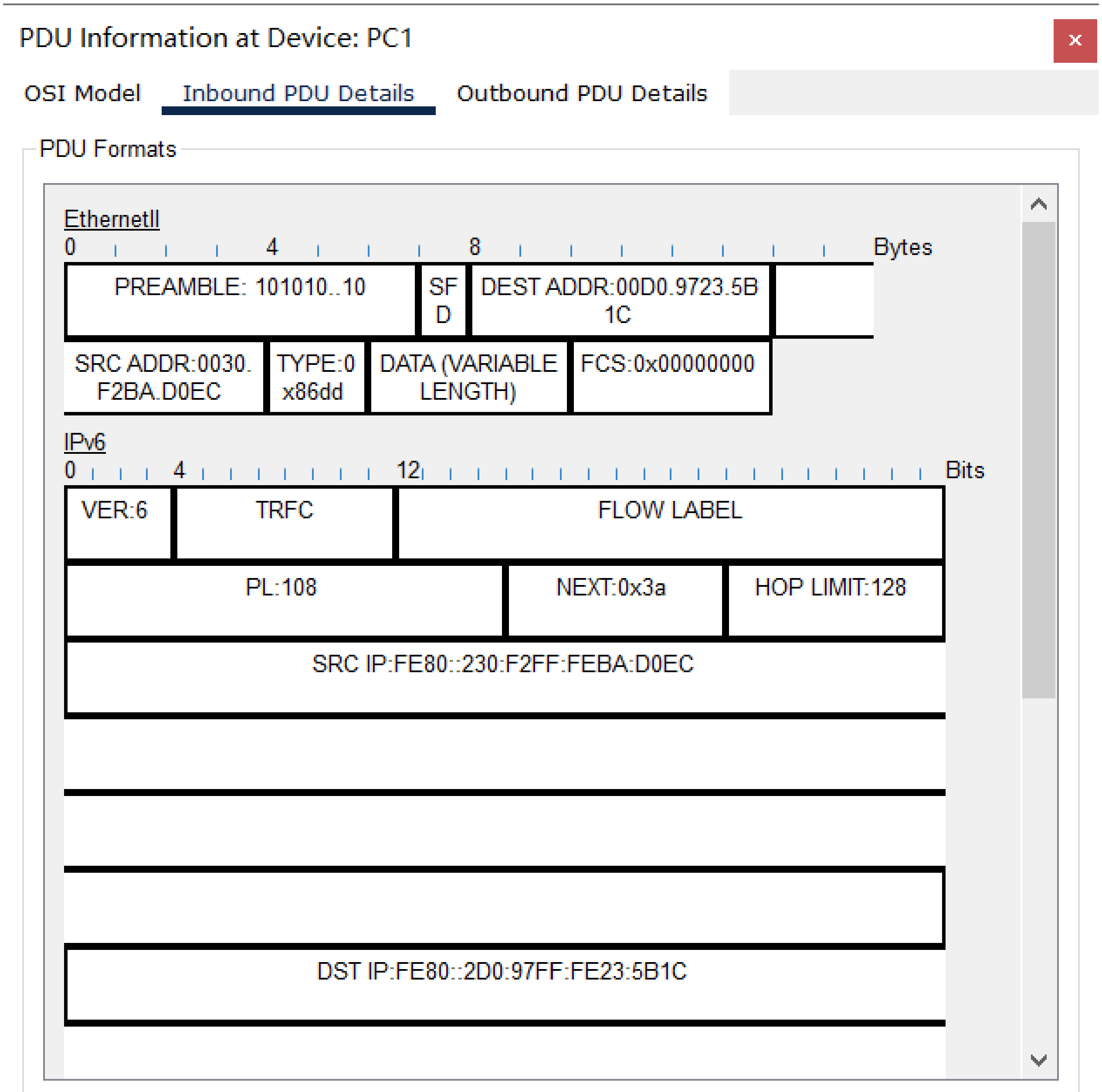
A2: Open a command prompt and type the following commands:

```
ping FE80::2D0:97FF:FE23:5B1C
```

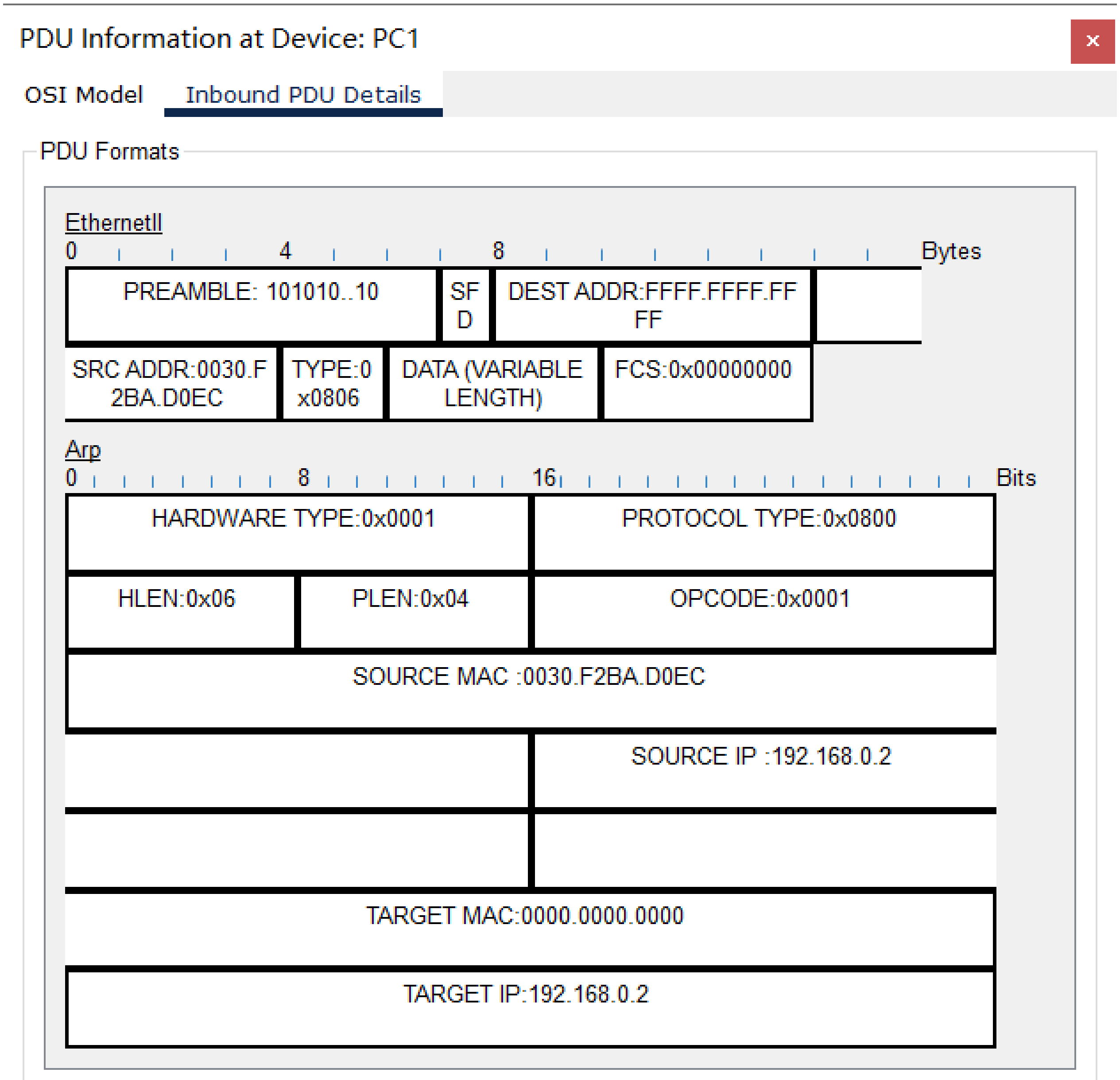


- Q3: What’s the difference between IPv4 datagram and IPv6 datagram? List at least 3 aspects.

A3: get the ipv6 packet under the simulation mode:



get the ipv4 packet under the simulation mode:



We can see there are several differences:

1. ipv6 contains hardware information, while ipv4 not
2. ipv6 omites the protocol type information
3. ipv6 omites opcde and adds hop limit in the datagram

- Q4: Does these two IPv6 addresses belong to the same sub-net, what is the sub-net ID of these two IPv6 addresses?

A4: use ipconfig to get the subnet mask.

> Subnet mask
> PC0: 255.255.255.0
> PC1: 255.255.255.0

> IP address
> PC0: 192.168.0.2
> PC1: 192.168.0.1

We do the AND operation between subnet mask and IP address. The result is same: 192.168.0.0

Thus they belong to the same sub-net, and their sub-net ID is 192.168.0.0.