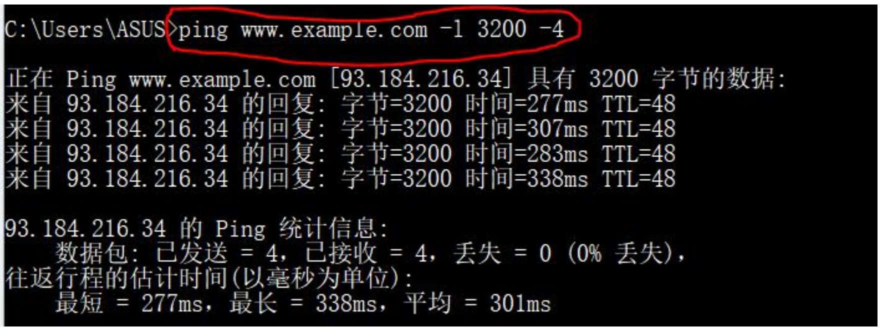
Std_ID: 11712325

Std_NAME: 张家毓

1. **Initiates an ICMP session to test if www.example.com is reachable(setting the packet size is 3200B), capture the packets.**

① How to initiates an ICMP Echo request with 3200B length?



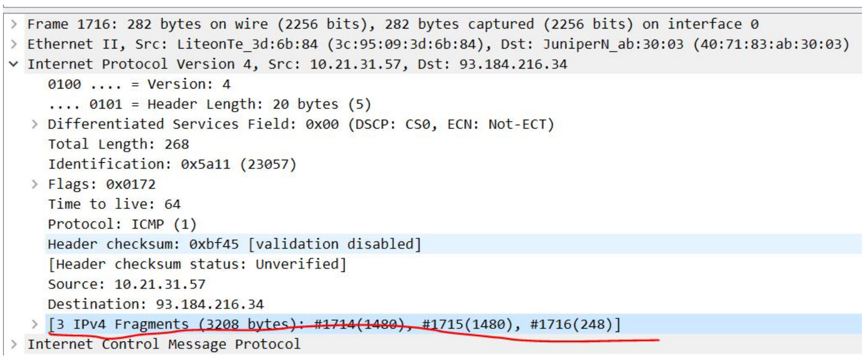
```
C:\Users\ASUS>ping www.example.com -l 3200 -4

正在 Ping www.example.com [93.184.216.34] 具有 3200 字节的数据:
来自 93.184.216.34 的回复: 字节=3200 时间=277ms TTL=48
来自 93.184.216.34 的回复: 字节=3200 时间=307ms TTL=48
来自 93.184.216.34 的回复: 字节=3200 时间=283ms TTL=48
来自 93.184.216.34 的回复: 字节=3200 时间=338ms TTL=48

93.184.216.34 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 = 277ms, 最长 = 338ms, 平均 = 301ms
```

fig.1

Command: ping www.example.com -l 3200 -4

② Is there any fragmentation on the IP packets , how do you find it ?

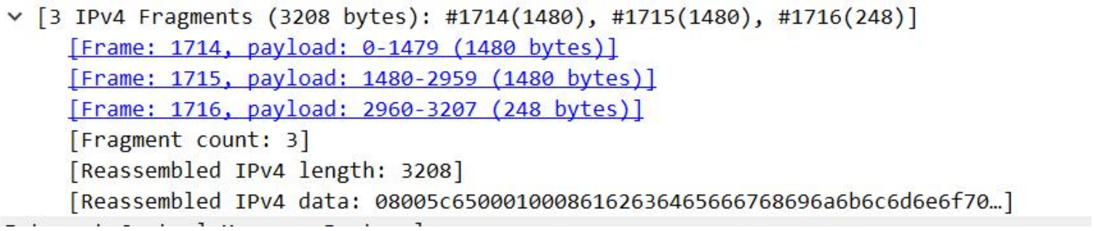
Yes.We can find them here.



```
> Frame 1716: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0
> Ethernet II, Src: LiteonTe_3d:6b:84 (3c:95:09:3d:6b:84), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
v Internet Protocol Version 4, Src: 10.21.31.57, Dst: 93.184.216.34
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 268
    Identification: 0x5a11 (23057)
  > Flags: 0x0172
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xbf45 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.21.31.57
    Destination: 93.184.216.34
  > [3 IPv4 Fragments (3208 bytes): #1714(1480), #1715(1480), #1716(248)]
> Internet Control Message Protocol
```

fig.2

③How many fragments of a 3200B length IP packet ?

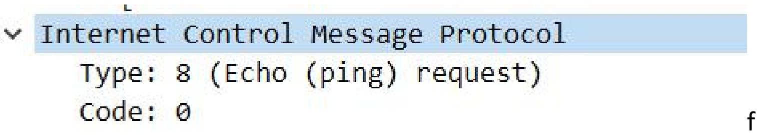


```
v [3 IPv4 Fragments (3208 bytes): #1714(1480), #1715(1480), #1716(248)]
    [Frame: 1714, payload: 0-1479 (1480 bytes)]
    [Frame: 1715, payload: 1480-2959 (1480 bytes)]
    [Frame: 1716, payload: 2960-3207 (248 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3208]
    [Reassembled IPv4 data: 08005c65000100086162636465666768696a6b6c6d6e6f70…]
```

fig.3

From fig.3,we can find there **3** fragments of a 3200B length IP packet.

④How do you identify the ICMP Echo request and Echo reply?

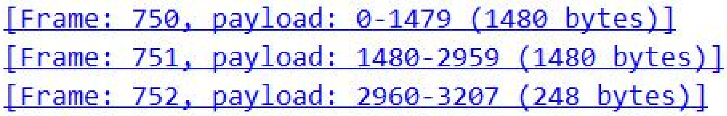


```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

fig.4

We can identify them in the information.

⑤For the ICMP Echo request, which fragment is the 1st one, which is the last ? How do you identify them?



```
[Frame: 750, payload: 0-1479 (1480 bytes)]
[Frame: 751, payload: 1480-2959 (1480 bytes)]
[Frame: 752, payload: 2960-3207 (248 bytes)]
```

fig.5

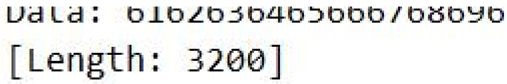
For example ， the first line of fig.5 is the first fragment.And the last line is the last fragment.I identify them by the scale of their payload .

⑥What’ s the length of each IP fragment? Is the sum of each fragment’ s length equal to the original IP packet ?

From fig.5 , we can know that , the length of

the first fragment is 1480 bytes,
The second fragment is 1480 bytes,
The third fragment is 248 bytes.

The sum of the fragments’ length is 1480 + 1480 + 248 = 3208 bytes.



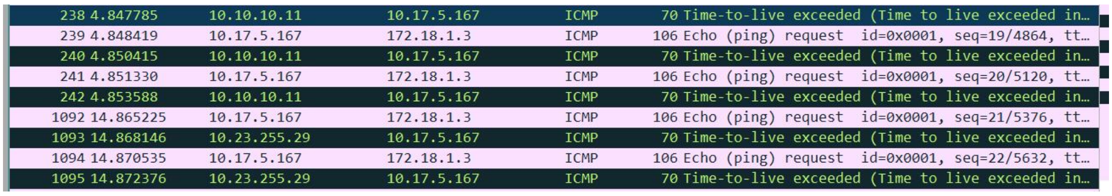
```
Data: 6162636465666768696
[Length: 3200]
```

fig.6

The original IP packet’s length is 3200.They are not equal.

2. using tracert (windows) / traceroute(linux or MacOS) to trace the route from your host to www.sustech.edu.cn.

① Is there any ‘Time-to-live exceeded’ ICMP packets?



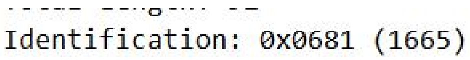
```
 238 4.847785   10.10.10.11    10.17.5.167   ICMP   70 Time-to-live exceeded (Time to live exceeded in…
 239 4.848419   10.17.5.167    172.18.1.3    ICMP  106 Echo (ping) request  id=0x0001, seq=19/4864, tt…
 240 4.850415   10.10.10.11    10.17.5.167   ICMP   70 Time-to-live exceeded (Time to live exceeded in…
 241 4.851330   10.17.5.167    172.18.1.3    ICMP  106 Echo (ping) request  id=0x0001, seq=20/5120, tt…
 242 4.853588   10.10.10.11    10.17.5.167   ICMP   70 Time-to-live exceeded (Time to live exceeded in…
1092 14.865225  10.17.5.167    172.18.1.3    ICMP  106 Echo (ping) request  id=0x0001, seq=21/5376, tt…
1093 14.868146  10.23.255.29   10.17.5.167   ICMP   70 Time-to-live exceeded (Time to live exceeded in…
1094 14.870535  10.17.5.167    172.18.1.3    ICMP  106 Echo (ping) request  id=0x0001, seq=22/5632, tt…
1095 14.872376  10.23.255.29   10.17.5.167   ICMP   70 Time-to-live exceeded (Time to live exceeded in…
```

fig.7

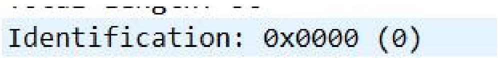
Yes,there are TTL exceed ICMP packets.

②what’s the difference between these packets and normal ICMP packets(such as ICMP echo request)? List at least 3 aspects.

（一）



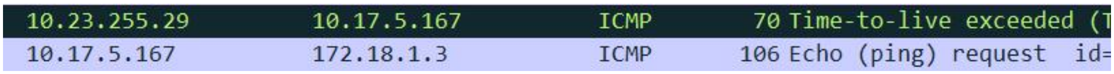
```
Identification: 0x0681 (1665)
```



```
Identification: 0x0000 (0)
```

in ttl exceed ICMP packets ,their identification is 0x0000. And in normal echo request packets , the identification is not 0x0000.

（二）



```
10.23.255.29    10.17.5.167    ICMP    70 Time-to-live exceeded (T
10.17.5.167     172.18.1.3     ICMP   106 Echo (ping) request  id=
```

fig.8 .

We can see in the exceed ICMP packets, their src ip all are 10.17.5.167, dst ip is 10.17.5.167

And the normal echo request ICMP packets ,their src ip all are 10.17.5.167 , dst ip is 172.18.1.3.

（三）

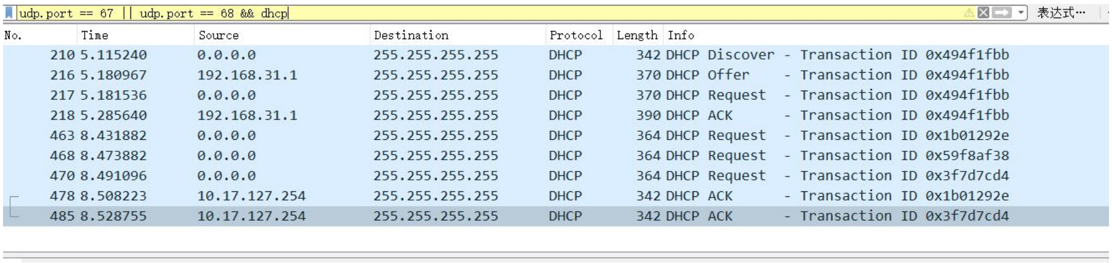
```
Total Length: 92
```

```
Total Length: 56
```

In ttl exceed ICMP packets , the total length all are 92. In normal echo request ICMP packets , the total packets are all 56.

3. Initiates a DHCP session

①How to initiate a DHCP session? How to find the DHCP session packets?



```
udp.port == 67 || udp.port == 68 && dhcp
No.     Time          Source            Destination        Protocol  Length Info
    210 5.115240      0.0.0.0           255.255.255.255    DHCP      342 DHCP Discover - Transaction ID 0x494f1fbb
    216 5.180967      192.168.31.1      255.255.255.255    DHCP      370 DHCP Offer    - Transaction ID 0x494f1fbb
    217 5.181536      0.0.0.0           255.255.255.255    DHCP      370 DHCP Request  - Transaction ID 0x494f1fbb
    218 5.285640      192.168.31.1      255.255.255.255    DHCP      390 DHCP ACK      - Transaction ID 0x494f1fbb
    463 8.431882      0.0.0.0           255.255.255.255    DHCP      364 DHCP Request  - Transaction ID 0x1b01292e
    468 8.473882      0.0.0.0           255.255.255.255    DHCP      364 DHCP Request  - Transaction ID 0x59f8af38
    470 8.491096      0.0.0.0           255.255.255.255    DHCP      364 DHCP Request  - Transaction ID 0x3f7d7cd4
    478 8.508223      10.17.127.254     255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x1b01292e
    485 8.528755      10.17.127.254     255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x3f7d7cd4
```

fig.8

Close the network and reconnect the network.

Use the filter command: **udp.port == 67 || udp.port == 68 && dhcp.**

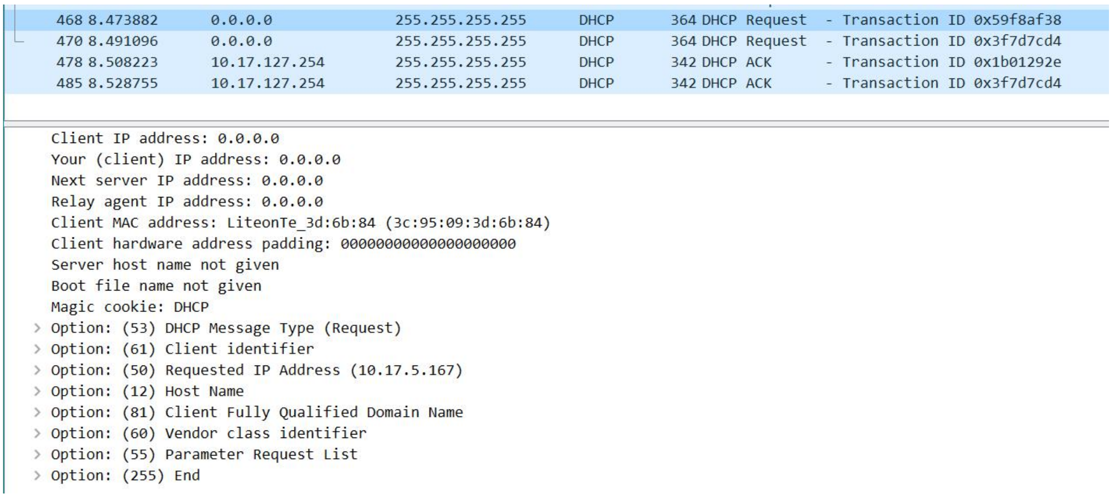
②What ‘s the source IP address and destination IP address of a DHCP request? What is the type of these two IP address?

Source address : 0.0.0.0

Destination address : 255.255.255.255

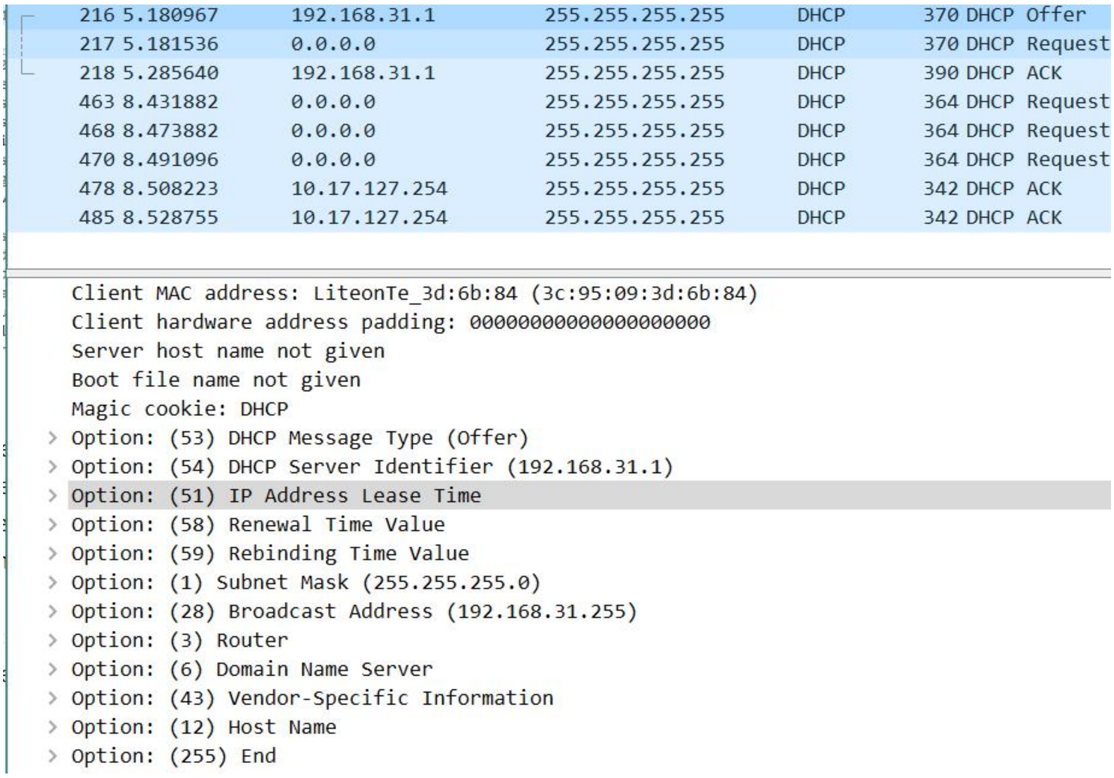
Type: ipv4

③What info items are required for a host if it need to contact with others in the Internet?



```
    468 8.473882      0.0.0.0           255.255.255.255    DHCP      364 DHCP Request  - Transaction ID 0x59f8af38
    470 8.491096      0.0.0.0           255.255.255.255    DHCP      364 DHCP Request  - Transaction ID 0x3f7d7cd4
    478 8.508223      10.17.127.254     255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x1b01292e
    485 8.528755      10.17.127.254     255.255.255.255    DHCP      342 DHCP ACK      - Transaction ID 0x3f7d7cd4

    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_3d:6b:84 (3c:95:09:3d:6b:84)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (10.17.5.167)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

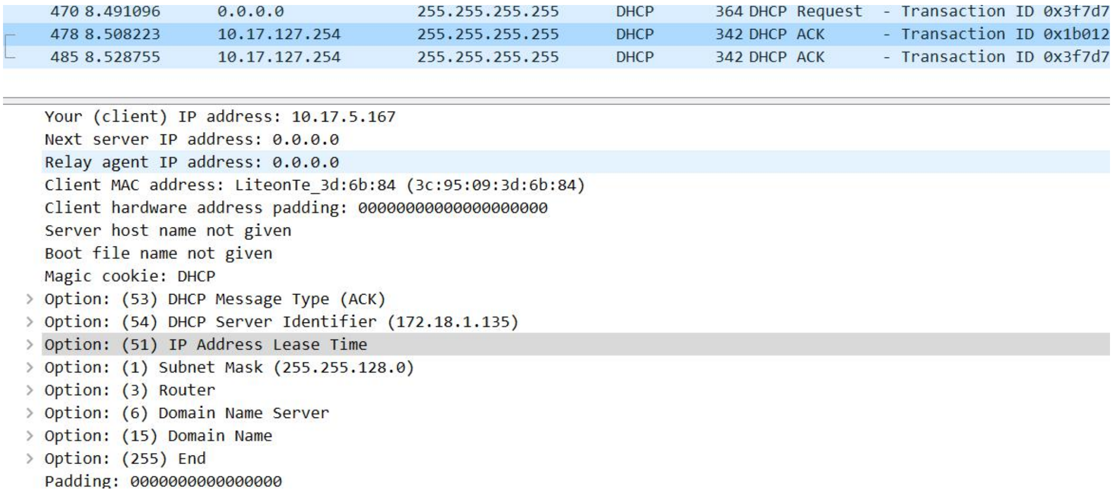
fig.9



```
216 5.180967    192.168.31.1     255.255.255.255    DHCP    370 DHCP Offer
217 5.181536    0.0.0.0          255.255.255.255    DHCP    370 DHCP Request
218 5.285640    192.168.31.1     255.255.255.255    DHCP    390 DHCP ACK
463 8.431882    0.0.0.0          255.255.255.255    DHCP    364 DHCP Request
468 8.473882    0.0.0.0          255.255.255.255    DHCP    364 DHCP Request
470 8.491096    0.0.0.0          255.255.255.255    DHCP    364 DHCP Request
478 8.508223    10.17.127.254    255.255.255.255    DHCP    342 DHCP ACK
485 8.528755    10.17.127.254    255.255.255.255    DHCP    342 DHCP ACK
```

```
    Client MAC address: LiteonTe_3d:6b:84 (3c:95:09:3d:6b:84)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.31.1)
  > Option: (51) IP Address Lease Time
  > Option: (58) Renewal Time Value
  > Option: (59) Rebinding Time Value
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (28) Broadcast Address (192.168.31.255)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (43) Vendor-Specific Information
  > Option: (12) Host Name
  > Option: (255) End
```

Fig.10



```
470 8.491096    0.0.0.0          255.255.255.255    DHCP    364 DHCP Request   - Transaction ID 0x3f7d7
478 8.508223    10.17.127.254    255.255.255.255    DHCP    342 DHCP ACK       - Transaction ID 0x1b012
485 8.528755    10.17.127.254    255.255.255.255    DHCP    342 DHCP ACK       - Transaction ID 0x3f7d7
```

```
    Your (client) IP address: 10.17.5.167
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: LiteonTe_3d:6b:84 (3c:95:09:3d:6b:84)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (54) DHCP Server Identifier (172.18.1.135)
  > Option: (51) IP Address Lease Time
  > Option: (1) Subnet Mask (255.255.128.0)
  > Option: (3) Router
  > Option: (6) Domain Name Server
  > Option: (15) Domain Name
  > Option: (255) End
    Padding: 0000000000000000
```

fig.11

Option(53): DHCP Message Type

Option(61): Client identifier

Option(51): ip address lease time

Option(3): Router

Option(15): Domain Name

Option(6):Domain Name Server

Option(50): Requested IP Address

Option(12): Host Name

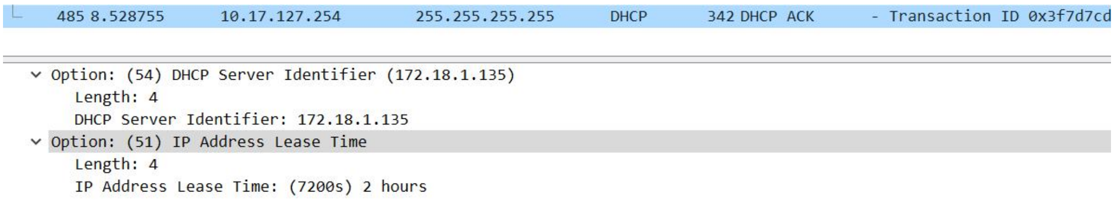
Option(81): Client Fully Qualified Domain Name

Option(60): Vendor class identifier

Option(55): Parameter Request List

Option(255): End

④How do you find the Lease Time of a dynamic IP address? What’s the value of it? In which type of DHCP packet could this field be set?



```
485 8.528755    10.17.127.254    255.255.255.255    DHCP    342 DHCP ACK    - Transaction ID 0x3f7d7cd

  ˅ Option: (54) DHCP Server Identifier (172.18.1.135)
        Length: 4
        DHCP Server Identifier: 172.18.1.135
  ˅ Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (7200s) 2 hours
```

fig.12

From fig.12 ,we can find it in Option(51).

The value is (7200s) 2 hours.

The type is ACK.