Southern University of Science and Technology

Computer Networking Lab Report

唐润哲 11710418

Assignment 10.1

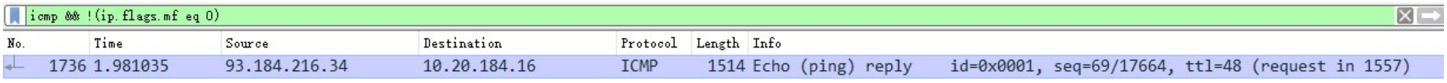
- ***Description***

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

1. How to initiate an ICMP Echo request with 3200B length?
2. Is there any fragmentation on the IP packets , how do you find it ?
3. How many fragments of a 3200B length IP packet ?
4. How do you identify the ICMP Echo request and Echo reply?
5. For the ICMP Echo request, which fragment is the 1st one, which is the last ? How do you identify them?
6. What’s the length of each IP fragment? Is the sum of eachfragment’s length equal to the original IP packet ?

- ***Result***

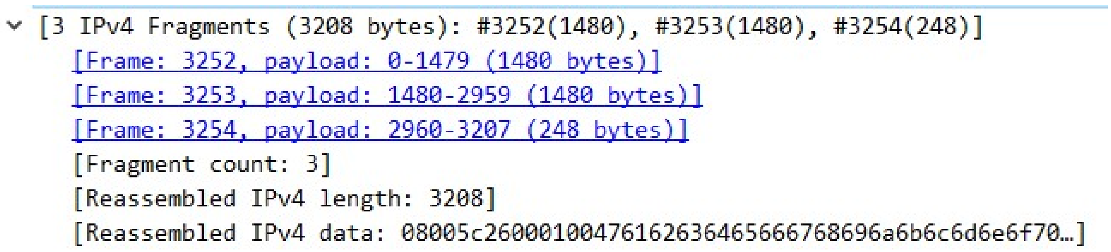
1. Command “ping -4 www.example.com -l 3200” is used to initiate an ICMP Echo request with 3200B length.
2. There is fragmentation on the IP packets, filter “icmp && !(ip.flags.mf eq 0)”is used to identify.



icmp && !(ip.flags.mf eq 0)

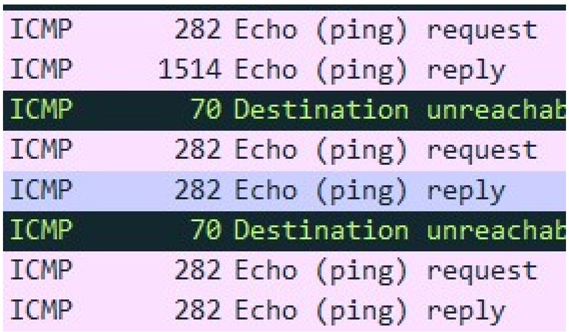
No.	Time	Source	Destination	Protocol	Length	Info
1736	1.981035	93.184.216.34	10.20.184.16	ICMP	1514	Echo (ping) reply id=0x0001, seq=69/17664, ttl=48 (request in 1557)

3. Three fragments are found.

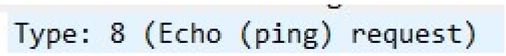


```
⌄ [3 IPv4 Fragments (3208 bytes): #3252(1480), #3253(1480), #3254(248)]
    [Frame: 3252, payload: 0-1479 (1480 bytes)]
    [Frame: 3253, payload: 1480-2959 (1480 bytes)]
    [Frame: 3254, payload: 2960-3207 (248 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3208]
    [Reassembled IPv4 data: 08005c26000100476162636465666768696a6b6c6d6e6f70…]
```

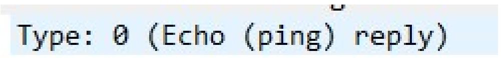
4. ICMP Echo request and Echo reply have different type number,8: Echo request,0: Echo reply. They are shown in the packet info.



```
ICMP       282 Echo (ping) request
ICMP      1514 Echo (ping) reply
ICMP        70 Destination unreachab
ICMP       282 Echo (ping) request
ICMP       282 Echo (ping) reply
ICMP        70 Destination unreachab
ICMP       282 Echo (ping) request
ICMP       282 Echo (ping) reply
```

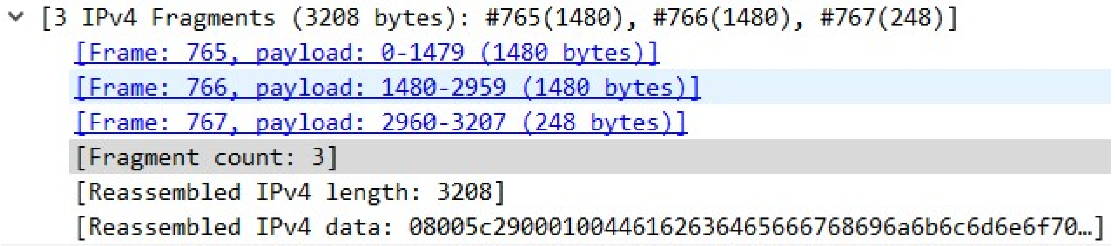


```
Type: 8 (Echo (ping) request)
```



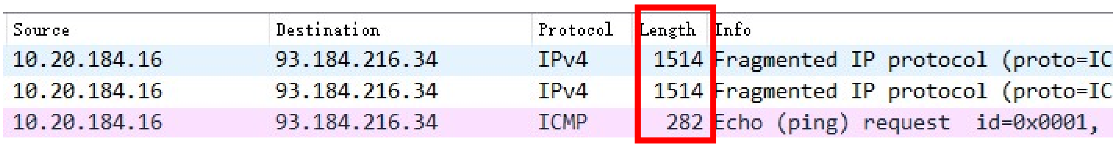
```
Type: 0 (Echo (ping) reply)
```

5. Identify them by the payload, the 1st and 2nd packet must be full and larger than or equal to the last packet, and the 3rd packet has the least data, so the Fragment #765 is the 1st one, Fragment #767 is the last one.



```
⌄ [3 IPv4 Fragments (3208 bytes): #765(1480), #766(1480), #767(248)]
    [Frame: 765, payload: 0-1479 (1480 bytes)]
    [Frame: 766, payload: 1480-2959 (1480 bytes)]
    [Frame: 767, payload: 2960-3207 (248 bytes)]
    [Fragment count: 3]
    [Reassembled IPv4 length: 3208]
    [Reassembled IPv4 data: 08005c29000100446162636465666768696a6b6c6d6e6f70…]
```

6. The length of each IP fragment is 1514+1514+282=3310. The length of original IP packet is 3200+20(IP header)+8(ICMP header)=3228. They are not equal.



Source	Destination	Protocol	Length	Info
10.20.184.16	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=IC
10.20.184.16	93.184.216.34	IPv4	1514	Fragmented IP protocol (proto=IC
10.20.184.16	93.184.216.34	ICMP	282	Echo (ping) request id=0x0001,

Assignment 10.2

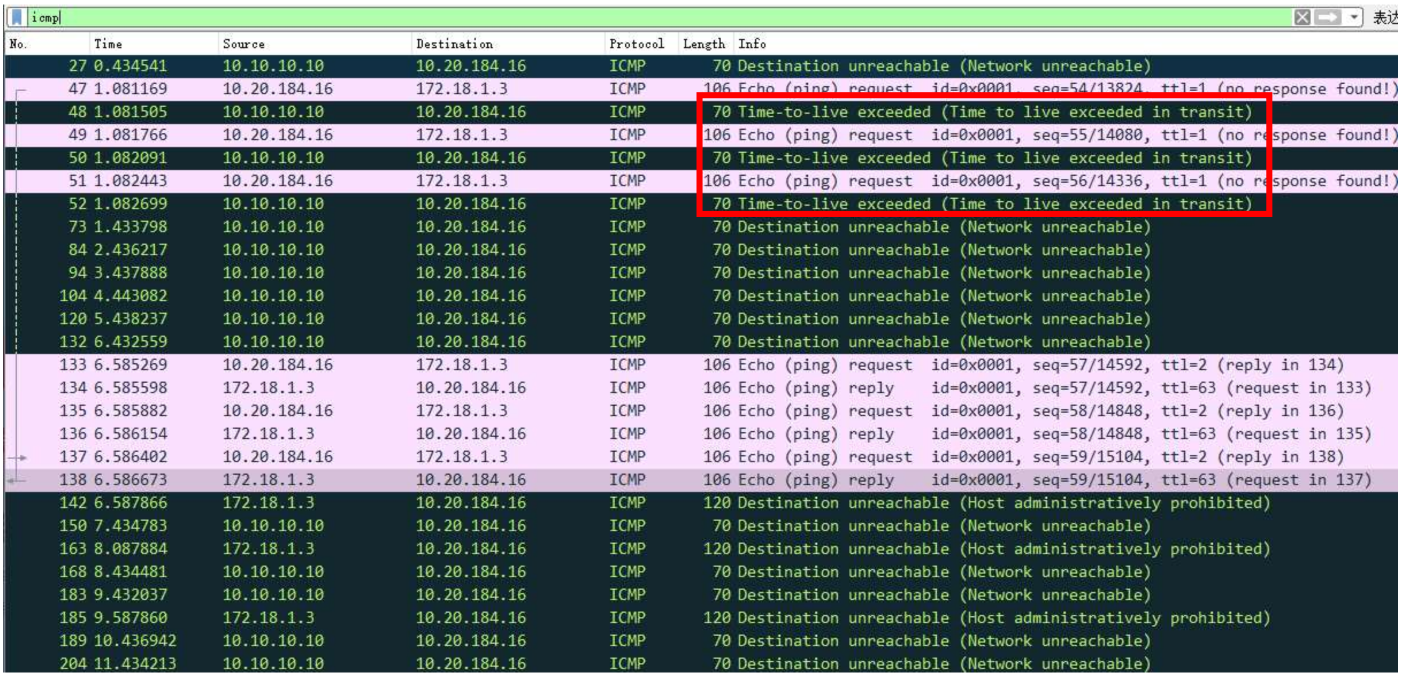
- ***Description***

Using tracert (windows) / traceroute(linux or MacOS) to trace the route from your host to www.sustech.edu.cn,capture the packets while tracing

1. Is there any ‘Time-to-live exceeded’ ICMP packets ?
2. What’s the difference between these packets and normal ICMP packets(such as ICMP echo request)? List at least 3 aspects.

- ***Result***

1. There are serval “Time-to-live exceeded” ICMP packets

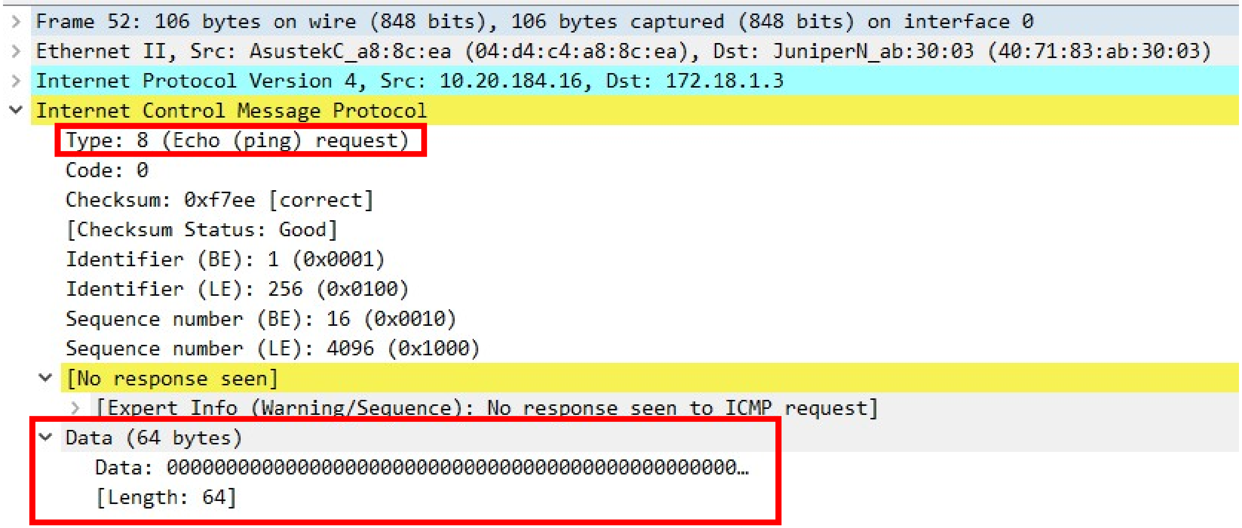


```
icmp
No.   Time       Source         Destination    Protocol Length Info
   27 0.434541   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
   47 1.081169   10.20.184.16   172.18.1.3     ICMP     106 Echo (ping) request  id=0x0001, seq=54/13824, ttl=1 (no response found!)
   48 1.081505   10.10.10.10    10.20.184.16   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   49 1.081766   10.20.184.16   172.18.1.3     ICMP     106 Echo (ping) request  id=0x0001, seq=55/14080, ttl=1 (no response found!)
   50 1.082091   10.10.10.10    10.20.184.16   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   51 1.082443   10.20.184.16   172.18.1.3     ICMP     106 Echo (ping) request  id=0x0001, seq=56/14336, ttl=1 (no response found!)
   52 1.082699   10.10.10.10    10.20.184.16   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   73 1.433798   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
   84 2.436217   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
   94 3.437888   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  104 4.443082   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  120 5.438237   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  132 6.432559   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  133 6.585269   10.20.184.16   172.18.1.3     ICMP     106 Echo (ping) request  id=0x0001, seq=57/14592, ttl=2 (reply in 134)
  134 6.585598   172.18.1.3     10.20.184.16   ICMP     106 Echo (ping) reply    id=0x0001, seq=57/14592, ttl=63 (request in 133)
  135 6.585882   10.20.184.16   172.18.1.3     ICMP     106 Echo (ping) request  id=0x0001, seq=58/14848, ttl=2 (reply in 136)
  136 6.586154   172.18.1.3     10.20.184.16   ICMP     106 Echo (ping) reply    id=0x0001, seq=58/14848, ttl=63 (request in 135)
  137 6.586402   10.20.184.16   172.18.1.3     ICMP     106 Echo (ping) request  id=0x0001, seq=59/15104, ttl=2 (reply in 138)
  138 6.586673   172.18.1.3     10.20.184.16   ICMP     106 Echo (ping) reply    id=0x0001, seq=59/15104, ttl=63 (request in 137)
  142 6.587866   172.18.1.3     10.20.184.16   ICMP     120 Destination unreachable (Host administratively prohibited)
  150 7.434783   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  163 8.087884   172.18.1.3     10.20.184.16   ICMP     120 Destination unreachable (Host administratively prohibited)
  168 8.434481   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  183 9.432037   10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  185 9.587860   172.18.1.3     10.20.184.16   ICMP     120 Destination unreachable (Host administratively prohibited)
  189 10.436942  10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
  204 11.434213  10.10.10.10    10.20.184.16   ICMP      70 Destination unreachable (Network unreachable)
```

2. ①Their ICMP types are different， 8 for normal,11 for ttl.

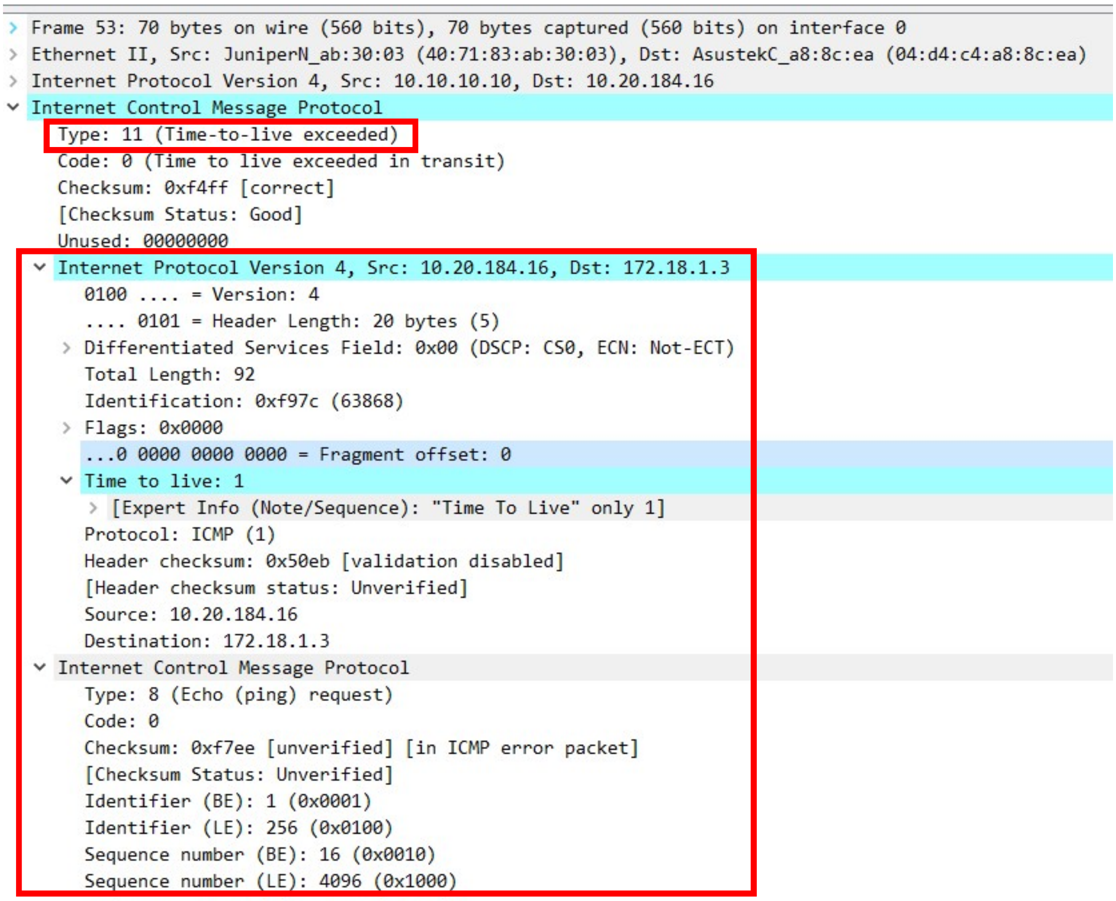
   ②The ttl packet includes a datagram from the ttl router/terminal.

   ③The normal packet has Data(64 bytes)



```
> Frame 52: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
> Internet Protocol Version 4, Src: 10.20.184.16, Dst: 172.18.1.3
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7ee [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 16 (0x0010)
    Sequence number (LE): 4096 (0x1000)
  v [No response seen]
    > [Expert Info (Warning/Sequence): No response seen to ICMP request]
  v Data (64 bytes)
      Data: 000000000000000000000000000000000000000000000000…
      [Length: 64]
```

normal ICMP packet



```
> Frame 53: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: JuniperN_ab:30:03 (40:71:83:ab:30:03), Dst: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea)
> Internet Protocol Version 4, Src: 10.10.10.10, Dst: 10.20.184.16
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
    Unused: 00000000
  v Internet Protocol Version 4, Src: 10.20.184.16, Dst: 172.18.1.3
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 92
      Identification: 0xf97c (63868)
    > Flags: 0x0000
      ...0 0000 0000 0000 = Fragment offset: 0
    v Time to live: 1
      > [Expert Info (Note/Sequence): "Time To Live" only 1]
      Protocol: ICMP (1)
      Header checksum: 0x50eb [validation disabled]
      [Header checksum status: Unverified]
      Source: 10.20.184.16
      Destination: 172.18.1.3
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf7ee [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence number (BE): 16 (0x0010)
      Sequence number (LE): 4096 (0x1000)
```

TTL-exceeded ICMP packet

Assignment 10.3

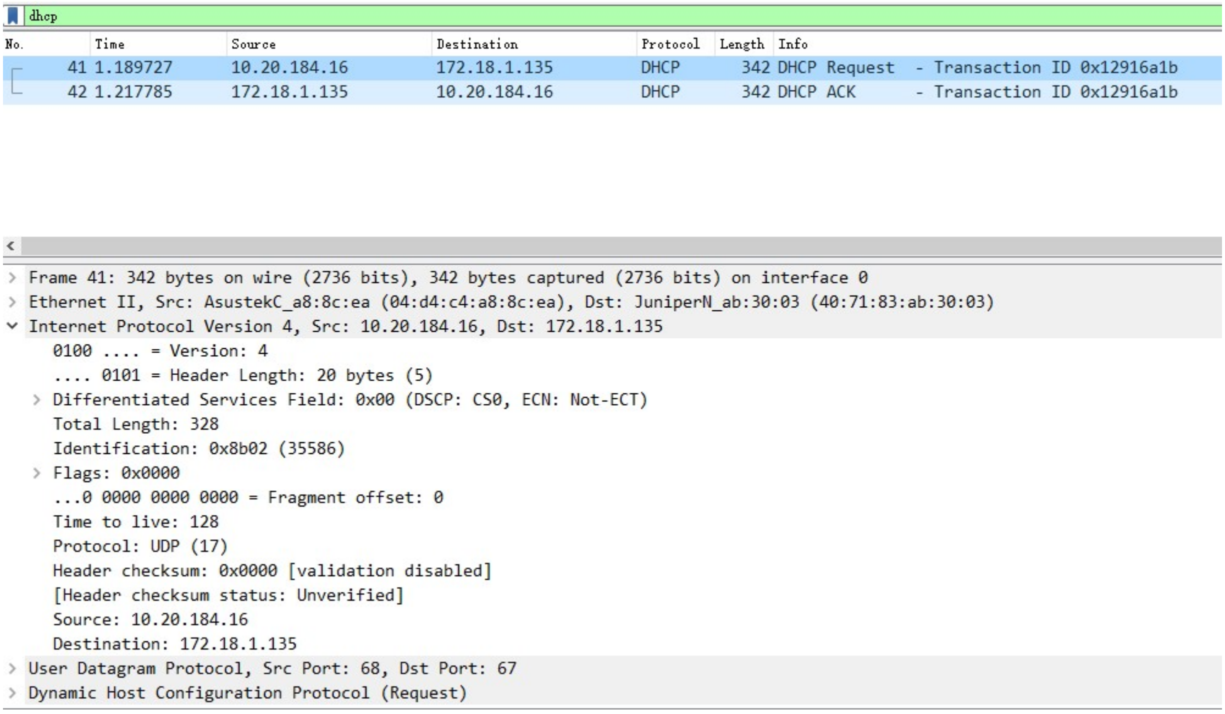
- ***Description***

Initiates a DHCP session

1. How to initiate a DHCP session? How to find the DHCP session packets?
2. What ‘s the source IP address and destination IP address of a DHCP request? What is the type of these two IP address?
3. What info items are required for a host if it need to contact with others in the Internet?
4. How 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?

- ***Result***

1. Command“ ipconfig -renew ”is used to initiate a DHCP session. Filter “dhcp” is used.



```
dhcp
No.     Time        Source          Destination     Protocol  Length  Info
     41 1.189727    10.20.184.16    172.18.1.135    DHCP         342  DHCP Request  - Transaction ID 0x12916a1b
     42 1.217785    172.18.1.135    10.20.184.16    DHCP         342  DHCP ACK      - Transaction ID 0x12916a1b
```

```
> Frame 41: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: AsustekC_a8:8c:ea (04:d4:c4:a8:8c:ea), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
v Internet Protocol Version 4, Src: 10.20.184.16, Dst: 172.18.1.135
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x8b02 (35586)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.20.184.16
    Destination: 172.18.1.135
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

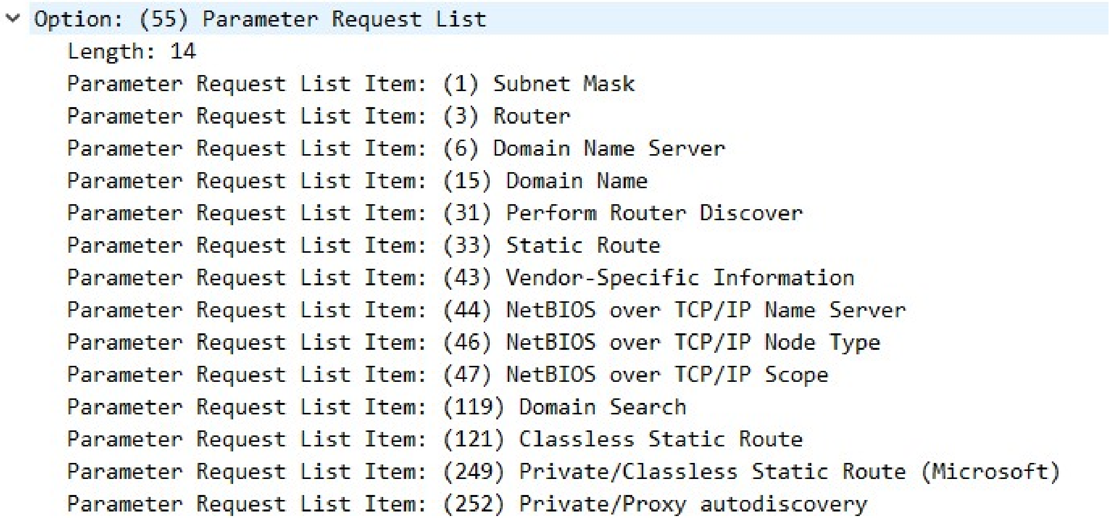
2. Source IP address :

   0.0.0.0 non-routable meta-address

   Destination IP address:

   255.255.255.255 broadcast address

3. Option: (55) includes all info items required.

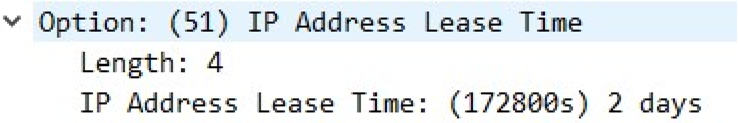


```
⌄ Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

4. Option: (51) IP Address Least Time.

   The value is 172800s=2days.

   Offer packet set the field.



```
⌄ Option: (51) IP Address Lease Time
    Length: 4
    IP Address Lease Time: (172800s) 2 days
```