

Lab10

Name: 胡玉斌

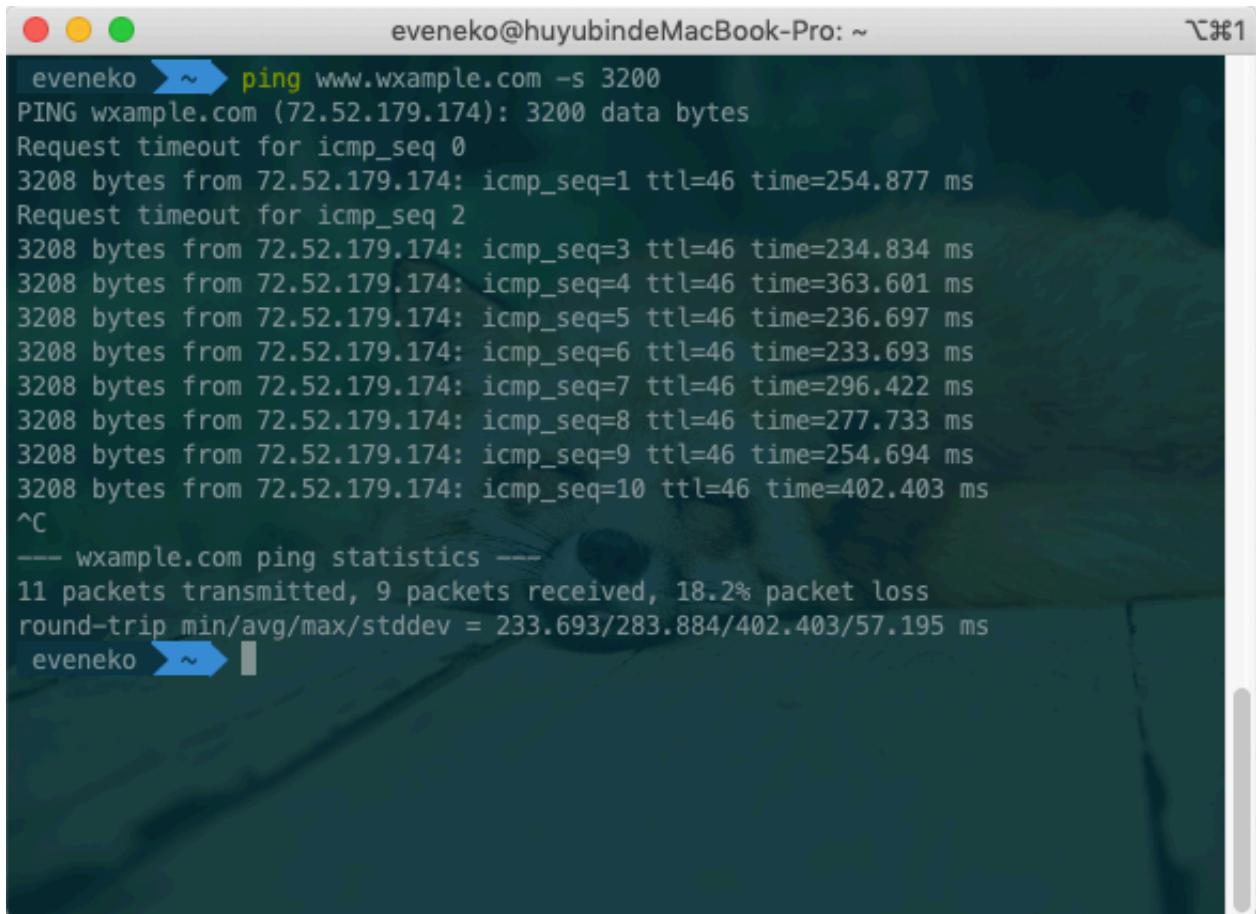
ID: 11712121

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

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

Using command `ping www.example.com -s 3200` for MAC

Using command `ping www.example.com -l 3200` for Win



```
eveneko@huyubindeMacBook-Pro: ~
eveneko ➤ ping www.wxample.com -s 3200
PING wxample.com (72.52.179.174): 3200 data bytes
Request timeout for icmp_seq 0
3208 bytes from 72.52.179.174: icmp_seq=1 ttl=46 time=254.877 ms
Request timeout for icmp_seq 2
3208 bytes from 72.52.179.174: icmp_seq=3 ttl=46 time=234.834 ms
3208 bytes from 72.52.179.174: icmp_seq=4 ttl=46 time=363.601 ms
3208 bytes from 72.52.179.174: icmp_seq=5 ttl=46 time=236.697 ms
3208 bytes from 72.52.179.174: icmp_seq=6 ttl=46 time=233.693 ms
3208 bytes from 72.52.179.174: icmp_seq=7 ttl=46 time=296.422 ms
3208 bytes from 72.52.179.174: icmp_seq=8 ttl=46 time=277.733 ms
3208 bytes from 72.52.179.174: icmp_seq=9 ttl=46 time=254.694 ms
3208 bytes from 72.52.179.174: icmp_seq=10 ttl=46 time=402.403 ms
^C
--- wxample.com ping statistics ---
11 packets transmitted, 9 packets received, 18.2% packet loss
round-trip min/avg/max/stddev = 233.693/283.884/402.403/57.195 ms
eveneko ➤ ~
```

Wireshark screenshot showing network traffic. A red box highlights the first few rows of the packet list.

No.	Time	Source	Destination	Protocol	Length/Info
1229	39.228970	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=4963) [Reassembled in #1231]
1181	38.588645	72.52.179.174	10.21.61.60	ICMP	282 Echo (ping) reply id=0xce2a, seq=4/1824, ttl=64 (request in 1155)
1188	38.588638	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a17a) [Reassembled in #1181]
1179	38.588242	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a17a) [Reassembled in #1181]
1155	38.225184	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=4/1824, ttl=64 (reply in 1181)
1154	38.225183	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=f79d) [Reassembled in #1155]
1153	38.225182	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=f79d) [Reassembled in #1155]
1120	37.457451	72.52.179.174	10.21.61.60	ICMP	282 Echo (ping) reply id=0xce2a, seq=3/768, ttl=46 (request in 1103)
1119	37.457447	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=9f8f) [Reassembled in #1120]
1118	37.457227	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=9f8f) [Reassembled in #1120]
1183	37.222743	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=3/768, ttl=64 (reply in 1120)
1182	37.222742	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=488d) [Reassembled in #1103]
1101	37.222741	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=488d) [Reassembled in #1103]
1064	36.217663	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=2/512, ttl=64 (no response found!)
1063	36.217662	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=5507) [Reassembled in #1064]
1062	36.217661	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5507) [Reassembled in #1064]
1811	35.469988	72.52.179.174	10.21.61.60	ICMP	1514 Echo (ping) reply id=0xce2a, seq=1/256, ttl=46 (request in 991)
1010	35.469986	72.52.179.174	10.21.61.60	IPv4	282 Fragmented IP protocol (proto=ICMP 1, off=0, ID=2960, ID=9b56) [Reassembled in #1011]
1009	35.469979	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=9b56) [Reassembled in #1011]
991	35.215308	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=1/256, ttl=64 (reply in 1011)
990	35.215308	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8e87) [Reassembled in #991]
989	35.215306	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8e87) [Reassembled in #991]
+ 965	34.210456	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=0/0, ttl=64 (no response found!)
+ 964	34.210456	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=9733) [Reassembled in #965]
+ 963	34.210455	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=9733) [Reassembled in #965]

Frame (282 bytes) Reassembled IPv4 (3208 bytes)

wireshark_Wi-Fi_2019119205716_Q3DHpl.pcapng

Packets: 44481 · Displayed: 60 (0.1%) · Profile: Default

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

Yes, there are some fragmentation on the IP packets.

In wireshark, it will mark them as "Fragment IP protocol"

Wireshark screenshot showing network traffic. A red box highlights the last few rows of the packet list.

No.	Time	Source	Destination	Protocol	Length/Info
1229	39.228970	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=4963) [Reassembled in #1231]
1181	38.588645	72.52.179.174	10.21.61.60	ICMP	282 Echo (ping) reply id=0xce2a, seq=4/1824, ttl=64 (request in 1155)
1188	38.588638	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=a17a) [Reassembled in #1181]
1179	38.588242	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=a17a) [Reassembled in #1181]
1155	38.225184	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=4/1824, ttl=64 (reply in 1181)
1154	38.225183	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=f79d) [Reassembled in #1155]
1153	38.225182	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=f79d) [Reassembled in #1155]
1120	37.457451	72.52.179.174	10.21.61.60	ICMP	282 Echo (ping) reply id=0xce2a, seq=3/768, ttl=46 (request in 1103)
1119	37.457447	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=9f8f) [Reassembled in #1120]
1118	37.457227	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=9f8f) [Reassembled in #1120]
1183	37.222743	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=3/768, ttl=64 (reply in 1120)
1182	37.222742	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=488d) [Reassembled in #1103]
1101	37.222741	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=488d) [Reassembled in #1103]
1064	36.217663	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=2/512, ttl=64 (no response found!)
1063	36.217662	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=5507) [Reassembled in #1064]
1062	36.217661	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=5507) [Reassembled in #1064]
1811	35.469988	72.52.179.174	10.21.61.60	ICMP	1514 Echo (ping) reply id=0xce2a, seq=1/256, ttl=46 (request in 991)
1010	35.469986	72.52.179.174	10.21.61.60	IPv4	282 Fragmented IP protocol (proto=ICMP 1, off=2960, ID=9b56) [Reassembled in #1011]
1009	35.469979	72.52.179.174	10.21.61.60	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=9b56) [Reassembled in #1011]
991	35.215308	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=1/256, ttl=64 (reply in 1011)
990	35.215308	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=8e87) [Reassembled in #991]
989	35.215306	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=8e87) [Reassembled in #991]
+ 965	34.210456	10.21.61.60	72.52.179.174	ICMP	282 Echo (ping) request id=0xce2a, seq=0/0, ttl=64 (no response found!)
+ 964	34.210456	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=9733) [Reassembled in #965]
+ 963	34.210455	10.21.61.60	72.52.179.174	IPv4	1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=9733) [Reassembled in #965]

Frame (282 bytes) Reassembled IPv4 (3208 bytes)

wireshark_Wi-Fi_2019119205716_Q3DHpl.pcapy

Packets: 41482 · Displayed: 60 (0.1%) · Profile: Default

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

Three fragments.

Wireshark Screenshot showing ICMP traffic between two hosts:

- Frame 965:** ICMP Echo request (Type 8) from 10.21.61.60 to 72.52.179.174.
- Frame 966:** ICMP Echo reply (Type 0) from 72.52.179.174 to 10.21.61.60.
- Frame 963:** ICMP Echo request (Type 8) from 10.21.61.60 to 72.52.179.174.
- Frame 964:** ICMP Echo reply (Type 0) from 72.52.179.174 to 10.21.61.60.

The frames are highlighted with red boxes in the timeline view.

Wireshark Screenshot showing ICMP traffic between two hosts:

- Frame 24:** ICMP Echo request (Type 8) from 10.21.61.60 to 72.52.179.174.
- Frame 25:** ICMP Echo reply (Type 0) from 72.52.179.174 to 10.21.61.60.
- Frame 26:** ICMP Echo request (Type 8) from 10.21.61.60 to 72.52.179.174.
- Frame 27:** ICMP Echo reply (Type 0) from 72.52.179.174 to 10.21.61.60.
- Frame 28:** ICMP Echo request (Type 8) from 10.21.61.60 to 72.52.179.174.
- Frame 29:** ICMP Echo reply (Type 0) from 72.52.179.174 to 10.21.61.60.

The frames are highlighted with red boxes in the timeline view.

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

In wireshark, it will specify whether it is a request message or reply message for ICMP segment information.

No.	Time	Source	Destination	Protocol	Length	Info
1031	35.469088	72.52.179.174	10.21.61.60	ICMP	1514	Echo (ping) reply id=0xce2a, seq=1/256, ttl=46 (request in 991)
1487	44.651515	72.52.179.174	10.21.61.60	ICMP	1514	Echo (ping) reply id=0xce2a, seq=18/2560, ttl=46 (request in 1466)
1120	37.457451	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=3/768, ttl=46 (request in 1103)
1181	38.588645	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=4/1024, ttl=46 (request in 1155)
1264	39.465513	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=5/1280, ttl=46 (request in 1231)
1300	40.467628	72.52.179.174	10.21.61.60	ICMP	1514	Echo (ping) reply id=0xce2a, seq=6/1536, ttl=46 (request in 1287)
1324	41.535131	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=7/1792, ttl=46 (request in 1311)
1385	42.518099	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=8/2048, ttl=46 (request in 1361)
1445	43.499549	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=9/2304, ttl=46 (request in 1411)
965	34.218045	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) request id=0xce2a, seq=0/0, ttl=64 (no response found!)
991	35.215388	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=1/256, ttl=64 (reply in 1031)
1466	44.249247	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=18/2560, ttl=64 (reply in 1487)
1864	36.217663	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=2/512, ttl=64 (no response found!)
1103	37.222743	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=3/768, ttl=64 (reply in 1120)
1155	38.225184	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=4/1024, ttl=64 (reply in 1181)
1231	39.228972	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=5/1280, ttl=64 (reply in 1264)
1287	40.234082	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=6/1536, ttl=64 (reply in 1300)
1311	41.238859	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=7/1792, ttl=64 (reply in 1324)
1361	42.240510	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=8/2048, ttl=64 (reply in 1385)
1411	43.245085	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=9/2304, ttl=64 (reply in 1445)
1181	37.222741	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4880) [Reassembled in #1103]
1229	39.228970	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4963) [Reassembled in #1231]
1409	43.245083	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5038) [Reassembled in #1411]
1062	36.217661	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5507) [Reassembled in #1064]
1359	42.240508	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5521) [Reassembled in #1361]

Frame 1466: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0
 ▶ Ethernet II, Src: f8:ff:c2:1a:b8:ad (f8:ff:c2:1a:b8:ad), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
 ▶ Internet Protocol Version 4, Src: 10.21.61.60, Dst: 72.52.179.174
 ▶ Internet Control Message Protocol

Frame (282 bytes) Reassembled IPv4 (3208 bytes)

wireshark_Wi-Fi_20191119205716_Q3DHpl.pcang

Packets: 28606 - Displayed: 60 (0.2%) Profile: Default

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

The first request is 965, the last request is 1466

The way to identify them: the first seq is 0/0, the last(10th) is 10/2560

No.	Time	Source	Destination	Protocol	Length	Info
1359	42.240508	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5521) [Reassembled in #1361]
1062	36.217661	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5587) [Reassembled in #1064]
1409	43.245083	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=5038) [Reassembled in #1411]
1229	39.228970	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4963) [Reassembled in #1231]
1181	37.222741	10.21.61.60	72.52.179.174	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=4880) [Reassembled in #1103]
1411	43.245085	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=9/2304, ttl=64 (reply in 1445)
1361	42.240510	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=8/2048, ttl=64 (reply in 1385)
1311	41.238859	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=7/1792, ttl=64 (reply in 1324)
1287	40.234082	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=6/1536, ttl=64 (reply in 1300)
1231	39.228972	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=5/1280, ttl=64 (reply in 1264)
1155	38.225184	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=4/1024, ttl=64 (reply in 1181)
1183	37.222743	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=3/768, ttl=64 (reply in 1120)
1064	36.217663	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=2/512, ttl=64 (no response found!)
1466	44.249247	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=18/2560, ttl=64 (reply in 1487)
991	35.215388	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=1/256, ttl=64 (no response found!)
965	34.210456	10.21.61.60	72.52.179.174	ICMP	282	Echo (ping) request id=0xce2a, seq=0/0, ttl=64 (no response found!)
1445	43.499549	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=9/2304, ttl=46 (request in 1411)
1385	42.518099	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=8/2048, ttl=46 (request in 1361)
1324	41.535131	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=7/1792, ttl=46 (request in 1311)
1300	40.467628	72.52.179.174	10.21.61.60	ICMP	1514	Echo (ping) reply id=0xce2a, seq=6/1536, ttl=46 (request in 1287)
1264	39.465513	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=5/1280, ttl=46 (request in 1231)
1181	38.588645	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=4/1024, ttl=46 (request in 1155)
1220	37.457451	72.52.179.174	10.21.61.60	ICMP	282	Echo (ping) reply id=0xce2a, seq=3/768, ttl=46 (request in 1103)
1487	44.651515	72.52.179.174	10.21.61.60	ICMP	1514	Echo (ping) reply id=0xce2a, seq=18/2560, ttl=46 (request in 1466)
1011	35.469988	72.52.179.174	10.21.61.60	ICMP	1514	Echo (ping) reply id=0xce2a, seq=1/256, ttl=46 (request in 991)

Frame 965: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0
 ▶ Ethernet II, Src: f8:ff:c2:1a:b8:ad (f8:ff:c2:1a:b8:ad), Dst: JuniperN_ab:30:03 (40:71:83:ab:30:03)
 ▶ Internet Protocol Version 4, Src: 10.21.61.60, Dst: 72.52.179.174
 ▶ Internet Control Message Protocol

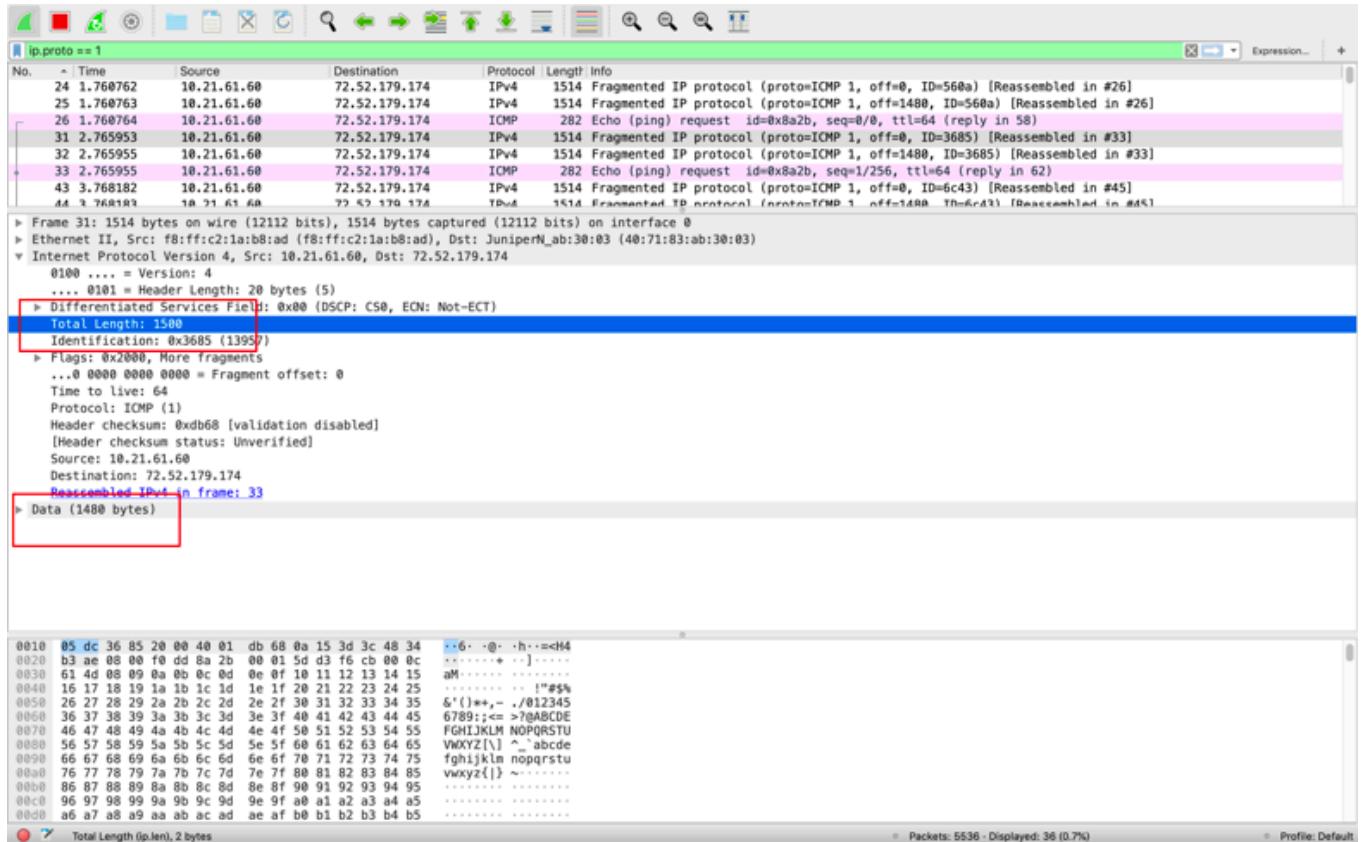
Frame (282 bytes) Reassembled IPv4 (3208 bytes)

wireshark_Wi-Fi_20191119205716_Q3DHpl.pcang

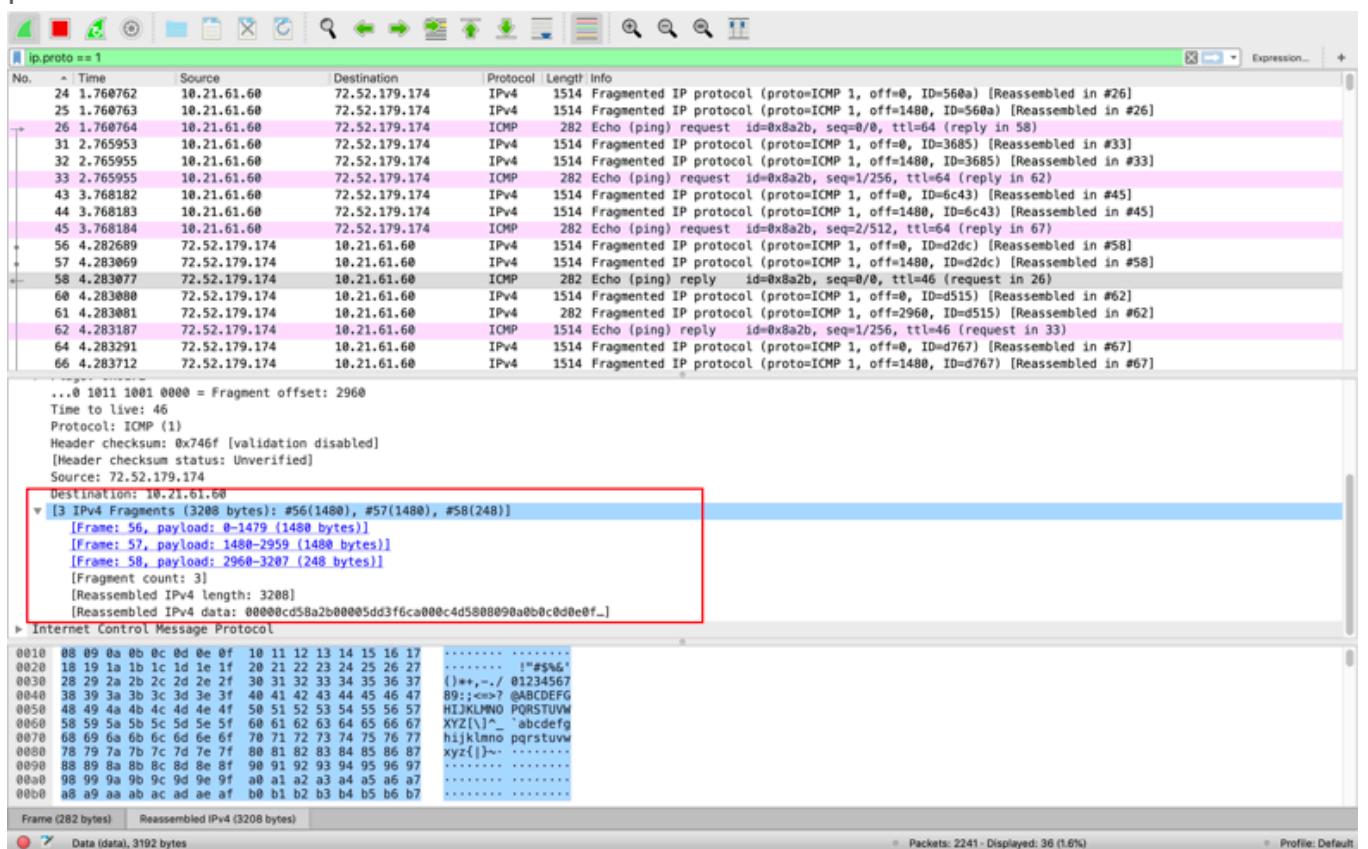
Packets: 48277 - Displayed: 60 (0.1%) Profile: Default

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

The Data is 1480 Bytes for the first and second fragment, the third is 248 Bytes, and the IP header is 20 Bytes. So the total length of each IP fragment is 1500 Bytes for the first and second fragment, the third is 268 Bytes.



No, The sum of each fragment's length is 3208 Bytes. It does not equal the original IP packet.



Please add the necessary screenshots and calculation when answering questions.

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

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

Yes, there are some 'Time-to-live exceeded' ICMP packets.

```
eveneko ~ traceroute www.sustech.edu.cn
traceroute to www.sustech.edu.cn (172.18.1.3), 64 hops max, 52 byte packets
 1  10.10.10.10 (10.10.10.10)  16.105 ms  5.063 ms  7.908 ms
 2  172.18.1.3 (172.18.1.3)  7.652 ms !Z  6.080 ms !Z  11.563 ms !Z
eveneko ~
```

No.	Time	Source	Destination	Protocol	Length	Info
45	1.5893415	10.10.10.10	10.21.61.60	ICMP	70	Time-to-live exceeded [Time to live exceeded in transit]
47	1.589102	10.10.10.10	10.21.61.60	ICMP	70	Time-to-live exceeded [Time to live exceeded in transit]
49	1.597047	10.10.10.10	10.21.61.60	ICMP	70	Time-to-live exceeded [Time to live exceeded in transit]
52	1.604702	172.18.1.3	10.21.61.60	ICMP	94	Destination unreachable (Host administratively prohibited)
54	1.611351	172.18.1.3	10.21.61.60	ICMP	94	Destination unreachable (Host administratively prohibited)
56	1.622958	172.18.1.3	10.21.61.60	ICMP	94	Destination unreachable (Host administratively prohibited)

Frame 45: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
Interface id: 0 (en0)
Interface name: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Nov 19, 2019 21:44:16.267260000 CST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1574171056.267260000 seconds
[Time delta from previous captured frame: 0.015856000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 1.583415000 seconds]
Frame Number: 45
Frame Length: 70 bytes (560 bits)
Capture Length: 70 bytes (560 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:ip:udp]
[Coloring Rule Name: ICMP errors]
[Coloring Rule String: icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv6.type eq 4]
0000 f8 ff c2 1a b8 ad 40 71 83 ab 30 03 08 00 45 00@q ..0..E.
0010 08 38 00 00 00 00 ff 01 60 60 0a 0a 0a 0a 15 .8.....
0020 3d 3c 00 00 e9 97 00 00 00 00 45 00 00 34 ab 52 =<..... E..4.R
0030 00 00 01 11 1a 01 0a 15 3d 3c ac 12 01 03 ab 51 =<...Q
0040 82 9b 00 20 dd 5a ... Z

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

Please add the necessary screenshots when answering questions.

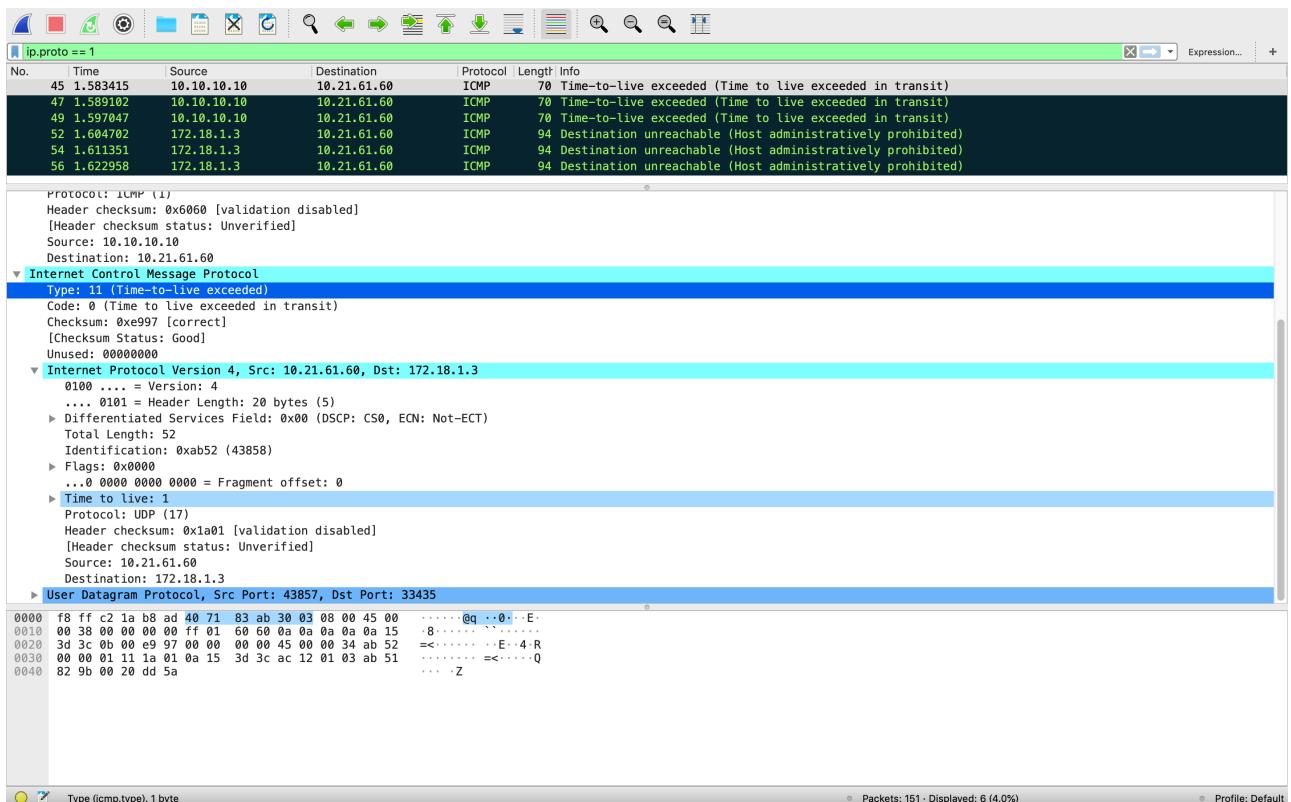
1. IP level identification

for these:

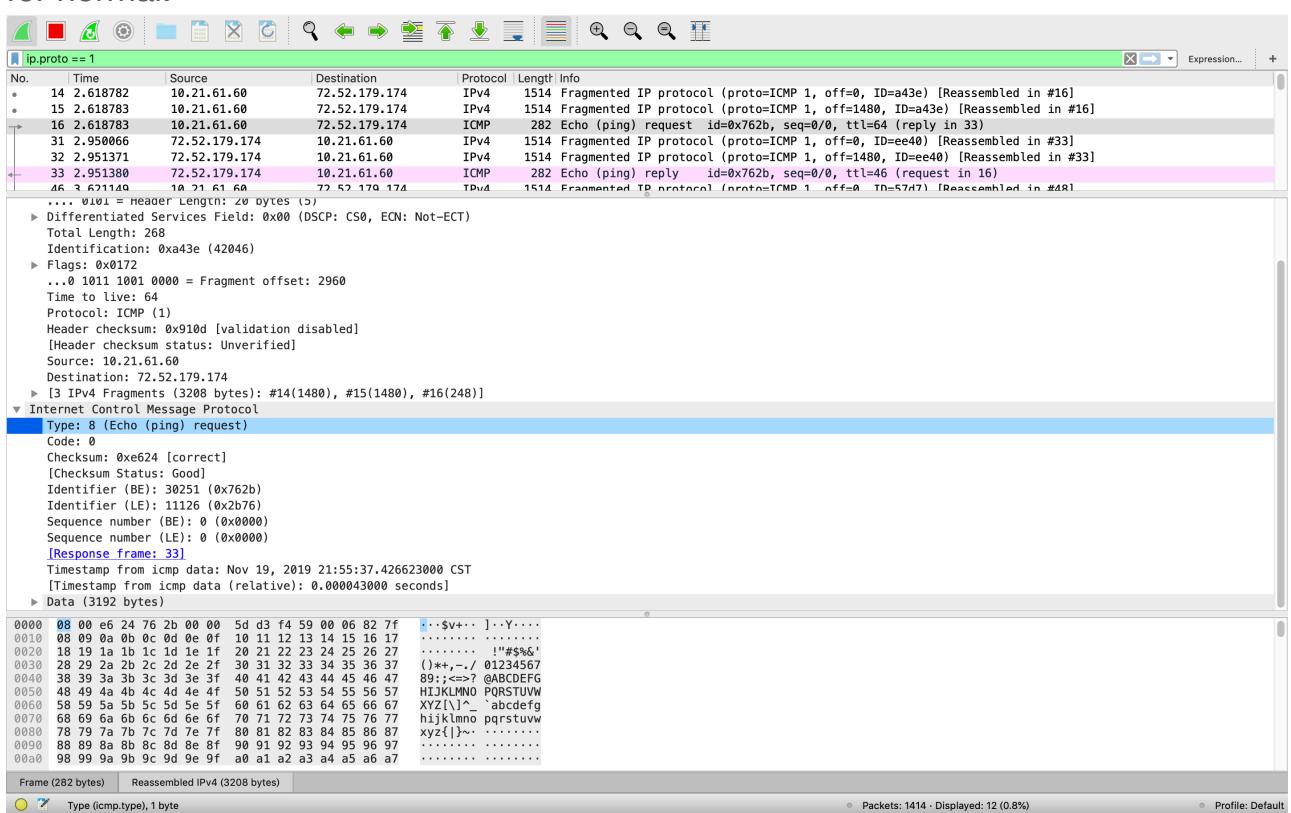
for normal:

2. ICMP level type:

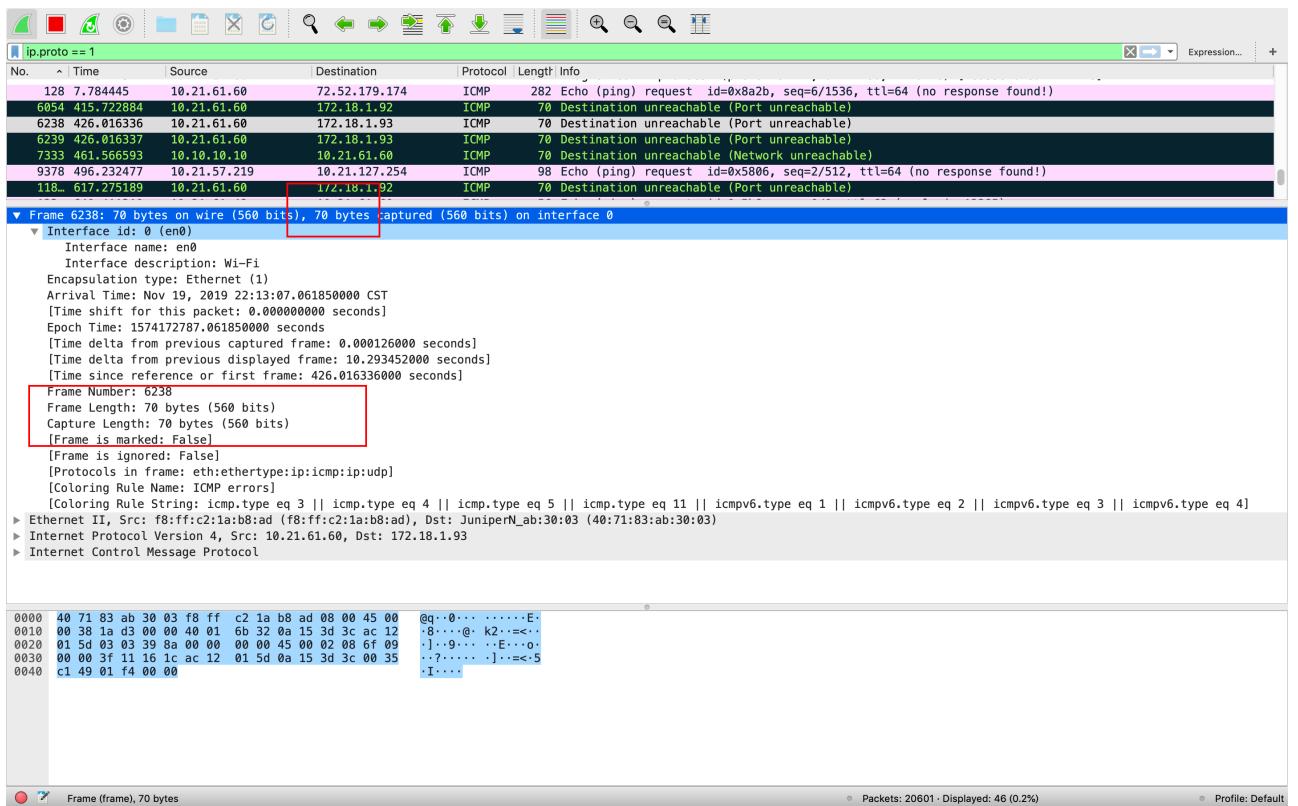
for these:



for normal:



3. The length, these packets are all 70 Bytes.



3. Initiates a DHCP session

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

Using command `ipconfig /release` to Remove the dynamic IP address for Win

Using command `ipconfig /renew` to Re-allocate IP address dynamically for Win
 display filter: `dhcp`

```
>ipconfig /release

Windows IP Configuration

No operation can be performed on 以太网 while it has its media disconnected.
No operation can be performed on 本地连接* 3 while it has its media disconnected.
No operation can be performed on 本地连接* 2 while it has its media disconnected.

Ethernet adapter 以太网:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter 本地连接* 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Wireless LAN adapter 本地连接* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::d05:f886:1689:b08e%7
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix . . .
    Link-local IPv6 Address . . . . . : fe80::f05f:87f9:4bc4:117f%11
    Default Gateway . . . . . :

Wireless LAN adapter WLAN:

    Connection-specific DNS Suffix . . .
    IPv6 Address. . . . . . . . . : 2001:da8:201d:1103:22c1:f7ab:3be3:65f2
    Link-local IPv6 Address . . . . . : fe80::193e:dcdf:7bb5:ea81%13
    Default Gateway . . . . . : fe80::4271:83ff:feab:3003%13
```

```
>ipconfig /renew
```

Windows IP Configuration

No operation can be performed on 以太网 while it has its media disconnected.
No operation can be performed on 本地连接* 3 while it has its media disconnected.
No operation can be performed on 本地连接* 2 while it has its media disconnected.

Ethernet adapter 以太网:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . .
```

Wireless LAN adapter 本地连接* 3:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . .
```

Wireless LAN adapter 本地连接* 2:

```
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . . .
```

Ethernet adapter VMware Network Adapter VMnet1:

```
Connection-specific DNS Suffix . . .  
Link-local IPv6 Address . . . . . : fe80::d05:f886:1689:b08e%7  
IPv4 Address. . . . . : 192.168.10.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

Ethernet adapter VMware Network Adapter VMnet8:

```
Connection-specific DNS Suffix . . .  
Link-local IPv6 Address . . . . . : fe80::f05f:87f9:4bc4:117f%11  
IPv4 Address. . . . . : 192.168.78.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :
```

Wireless LAN adapter WLAN:

```
Connection-specific DNS Suffix . . . : sustc.edu.cn  
IPv6 Address. . . . . : 2001:da8:201d:1103:22c1:f7ab:3be3:65f2  
Link-local IPv6 Address . . . . . : fe80::193e:dcdf:7bb5:ea81%13  
IPv4 Address. . . . . : 10.21.81.136  
Subnet Mask . . . . . : 255.255.128.0  
Default Gateway . . . . . : fe80::4271:83ff:feab:3003%13
```

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

For a DHCP request, the source IP address is 0.0.0.0 ,and the destination IP address is 255.255.255.255

Screenshot of Wireshark showing a DHCP session. The packet list shows several DHCP messages between a client (172.18.1.135) and a server (10.17.127.254). The details pane shows the configuration for the selected DHCP Request frame (Frame 2972). The bytes pane displays the raw hex and ASCII data of the selected frame.

No.	Time	Source	Destination	Protocol	Length	Info
152	1.332141	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380
259	2.785721	10.21.81.136	172.18.1.135	DHCP	342	DHCP Release - Transaction ID 0x56118569
430	4.444630	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380
1084	9.634975	10.21.127.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xd6d4ab70
1347	11.708464	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380
2838	22.987074	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe96d3594
2971	24.145147	10.21.127.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe96d3594
2972	24.146356	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe96d3594
3034	24.634966	10.21.127.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe96d3594
3400	27.187665	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380

Frame 2972: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface 0

Interface id: 0 (\Device\NPF_{5C93F5FB-4A07-4B73-B379-3EAD3F6074DF})
 Interface name: \Device\NPF_{5C93F5FB-4A07-4B73-B379-3EAD3F6074DF}
 Interface description: WLAN
 Encapsulation type: Ethernet (1)
 Arrival Time: Nov 19, 2019 22:35:47.698031000 CST
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1574174147.698031000 seconds
 [Time delta from previous captured frame: 0.001209000 seconds]
 [Time delta from previous displayed frame: 0.001209000 seconds]
 [Time since reference or first frame: 24.146356000 seconds]
 Frame Number: 2972
 Frame Length: 370 bytes (2960 bits)
 Capture Length: 370 bytes (2960 bits)
 [Frame is marked: False]
 [Frame is ignored: False]
 [Protocols in frame: eth:ethertype:ip:udp:dhcp]

0000 ff ff ff ff ff cc b0 da fd a0 af 08 00 45 00 E
 0010 01 64 6c 1e 00 80 11 cd 6b 00 00 00 00 ff ff ..d.....k...
 0020 ff ff 00 44 00 43 01 50 44 ff 01 01 06 00 e9 6d ..D C P D ..m
 0030 35 94 00 00 80 00 00 00 00 00 00 00 00 00 00 00 5...
 0040 00 00 00 00 00 00 00 cc b0 da fd a0 af 00 00 00 00
 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Frame (frame, 370 bytes) Packets: 4101 · Displayed: 10 (0.2%) Profile: Default

The address 0.0.0.0 is a non-routable meta-address used to designate an invalid, unknown or non-applicable target.

The address 255.255.255.255 is a broadcast address which is a network address at which all devices connected to a multiple-access communications network are enabled to receive datagrams

- What info items are required for a host if it need to contact with others in the Internet?
IP address, Subnet Mask, Default Gateway, DNS Server and Host Name
- 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?
Please add the necessary screenshots when answering questions.

In DHCP ACK to find the Lease Time

It is IP (172794s) 1 day, 23 hours, 59 minutes, 54 seconds

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
152	1.332141	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380
259	2.785721	10.21.81.136	172.18.1.135	DHCP	342	DHCP Release - Transaction ID 0x56118569
430	4.444630	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380
1084	9.634975	10.21.127.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xd6d4ab70
1347	11.708464	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380
2838	22.987074	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xe96d3594
2971	24.145147	10.21.127.254	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe96d3594
2972	24.146356	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xe96d3594
3034	24.634966	10.21.127.254	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe96d3594
3400	27.187665	172.18.1.135	10.17.127.254	DHCP	342	DHCP Offer - Transaction ID 0xd067e380

Magic cookie: DHCP

- ▼ Option: (53) DHCP Message Type (ACK)
 - Length: 1
 - DHCP: ACK (5)
- ▼ 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: (172794s) 1 day, 23 hours, 59 minutes, 54 seconds
- ▼ Option: (1) Subnet Mask (255.255.128.0)
 - Length: 4
 - Subnet Mask: 255.255.128.0
- ▼ Option: (3) Router
 - Length: 4
 - Router: 10.21.127.254
- ▼ Option: (6) Domain Name Server

0000	ff ff ff ff ff ff 40 71	83 ab 30 03 08 00 45 c0@q ..0 ..E
0010	01 48 00 00 00 00 ff 11	2f d2 0a 15 7f fe ff ff	H..... / ..
0020	ff ff 00 43 00 44 01 34	9c c5 02 01 06 01 d6 d4	..C ..D ..4 ..
0030	ab 70 00 00 80 00 00 00	00 00 0a 15 3d 67 00 00	p..... =g ..
0040	00 00 00 00 00 00 d0 c6	37 8d c3 68 00 00 00 00 7 ..h ..
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0070	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00b0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00c0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

Frame (frame), 342 bytes

Packets: 4101 · Displayed: 10 (0.2%) · Profile: Default