- School of Computer Science and Technology, Shandong University
- Lab Report on Computer Networking

Student Number	Name	Class	Lab Title	Period	Date
201900170249	李阳	智能19	ICMP v8.0	2h	May 25, 2021

Hardware Environment

- Lenovo Legion Y7000P 2020H(Intel Core i7-10750H, 16GB DDR4)
- Windows 10 Home, Chinese Version

Software Environment

- Wireshark-win64-3.44

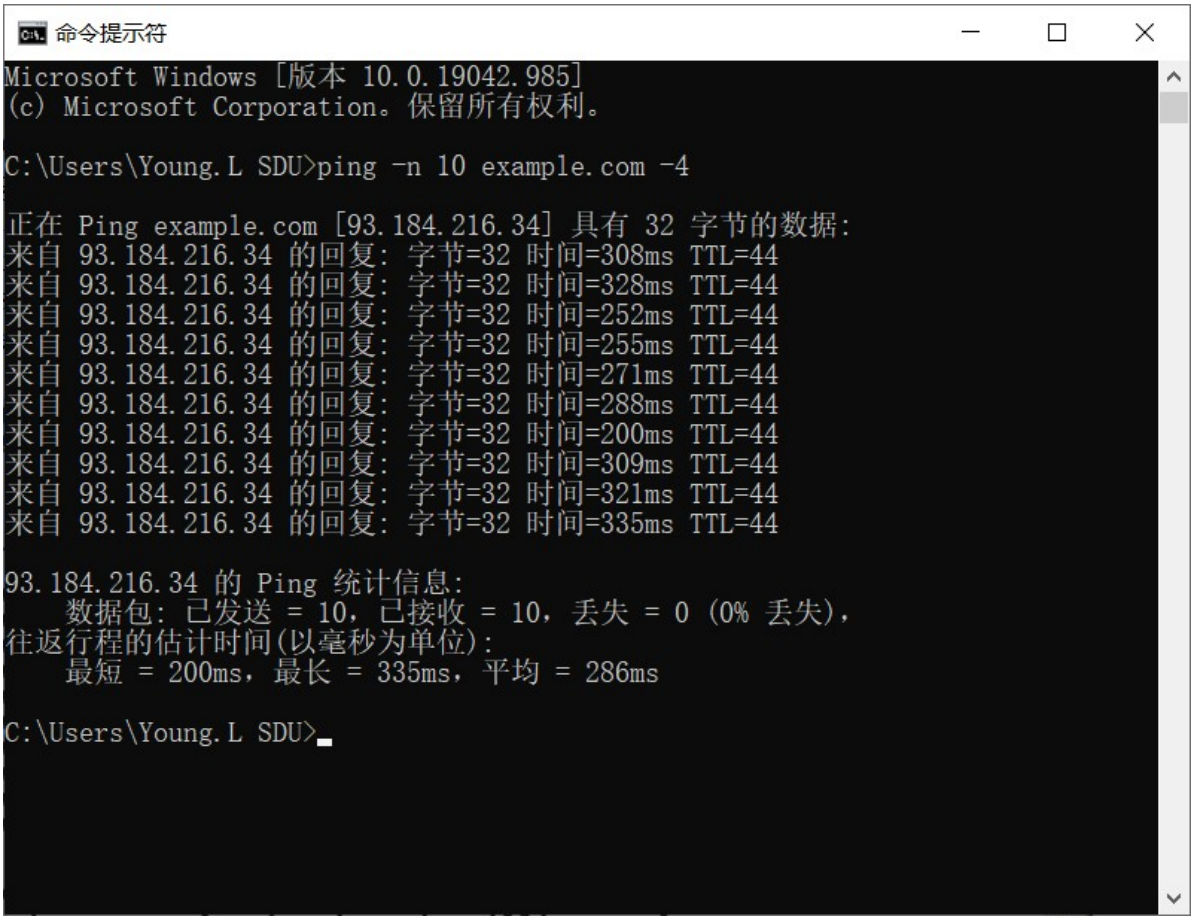
Purpose

- Explore ICMP messages generating by the Ping program.
- Explore ICMP messages generated by the Traceroute program.
- Explore the format and contents of an ICMP message.

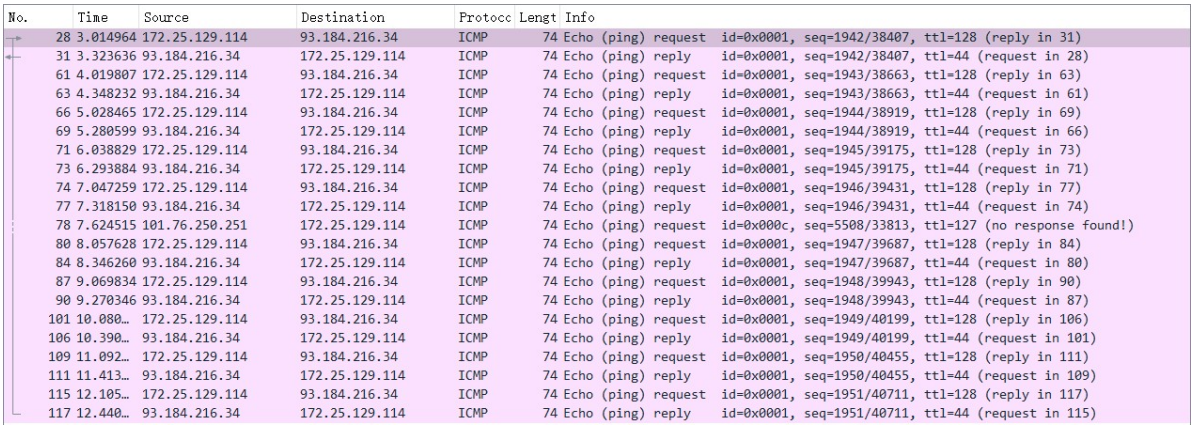
Experimental Records

ICMP and Ping

- Open the Windows Command Prompt application.
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- Type either "ping –n 10 hostname" or "C:\windows\system32\ping –n 10 hostname" in the MS-DOS command line, then run the Ping program by typing return. (hostname is a host on another continent)



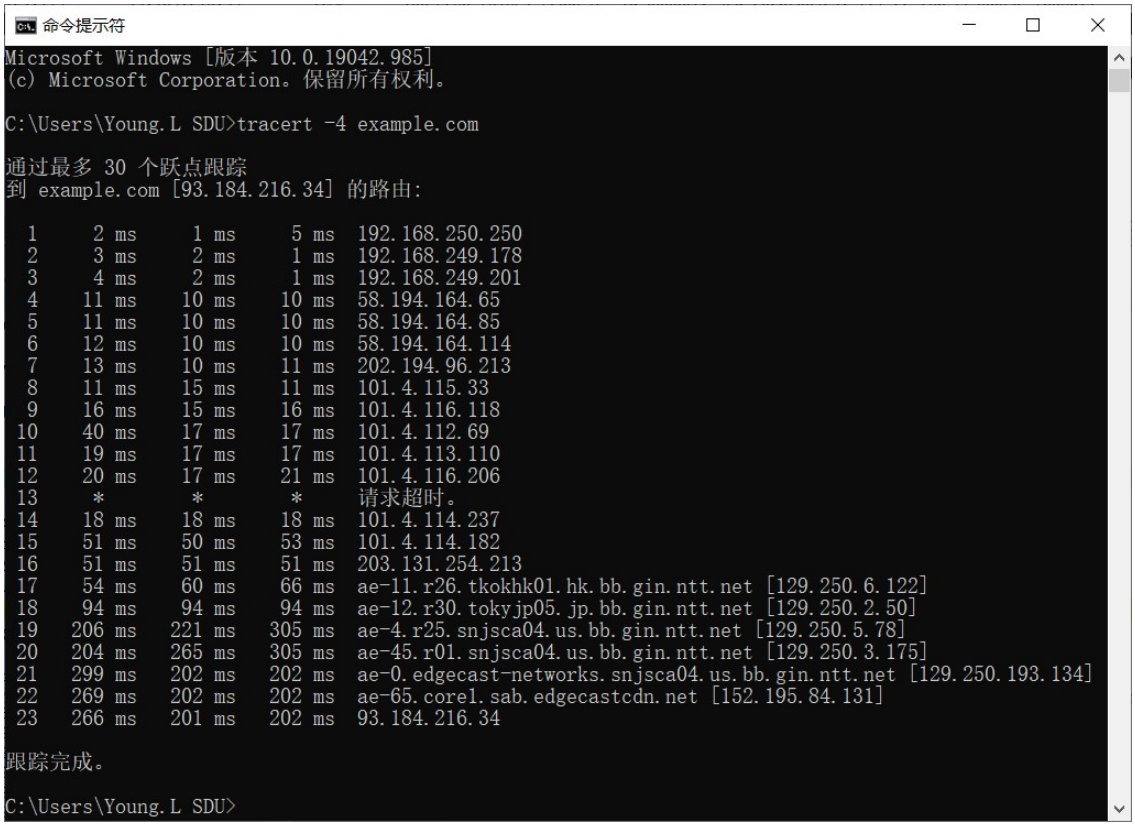
- When the Ping program terminates, stop the packet capture in Wireshark.



No.	Time	Source	Destination	Protocc	Lengt	Info
28	3.014964	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1942/38407, ttl=128 (reply in 31)
31	3.323636	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1942/38407, ttl=44 (request in 28)
61	4.019807	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1943/38663, ttl=128 (reply in 63)
63	4.348232	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1943/38663, ttl=44 (request in 61)
66	5.028465	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1944/38919, ttl=128 (reply in 69)
69	5.280599	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1944/38919, ttl=44 (request in 66)
71	6.038829	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1945/39175, ttl=128 (reply in 73)
73	6.293884	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1945/39175, ttl=44 (request in 71)
74	7.047259	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1946/39431, ttl=128 (reply in 77)
77	7.318150	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1946/39431, ttl=44 (request in 74)
78	7.624515	101.76.250.251	172.25.129.114	ICMP	74	Echo (ping) request id=0x000c, seq=5508/33813, ttl=127 (no response found!)
80	8.057628	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1947/39687, ttl=128 (reply in 84)
84	8.346260	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1947/39687, ttl=44 (request in 80)
87	9.069834	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1948/39943, ttl=128 (reply in 90)
90	9.270346	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1948/39943, ttl=44 (request in 87)
101	10.080…	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1949/40199, ttl=128 (reply in 106)
106	10.390…	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1949/40199, ttl=44 (request in 101)
109	11.092…	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1950/40455, ttl=128 (reply in 111)
111	11.413…	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1950/40455, ttl=44 (request in 109)
115	12.105…	172.25.129.114	93.184.216.34	ICMP	74	Echo (ping) request id=0x0001, seq=1951/40711, ttl=128 (reply in 117)
117	12.440…	93.184.216.34	172.25.129.114	ICMP	74	Echo (ping) reply id=0x0001, seq=1951/40711, ttl=44 (request in 115)

ICMP and Traceroute

- Open the Windows Command Prompt application.
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- Type either “tracert hostname” or “c:\windows\system32\tracert hostname” in the MS-DOS command line, where hostname is a host on another continent.



- When the Traceroute program terminates, stop packet capture in Wireshark.

Answer to Questions

1. The IP address of my host is 172.25.129.114, the IP address of destination host is 93.184.216.34.

```
Source Address: 172.25.129.114
Destination Address: 93.184.216.34
```

2. It was designed to communicate network-layer information between hosts and routers, not between application layer processes.

   Each ICMP packet has a "Type" and a "Code". The Type/Code combination identifies the specific message being received. Since the network software itself interprets all ICMP messages, no port numbers are needed to direct the ICMP message to an application layer process.

3. Type number is 8, code number is 0. The ICMP packet also has checksum, identifier, sequence number, and data fields. The checksum, sequence number and identifier fields are two bytes each.

```
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x45c5 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 1942 (0x0796)
Sequence Number (LE): 38407 (0x9607)
[Response frame: 31]
Data (32 bytes)
```

4. The ICMP type is 0, and the code number is 0. The ICMP packet has checksum, identifier, sequence number, data fields and response time. The checksum, sequence number and identifier fields are two bytes each.

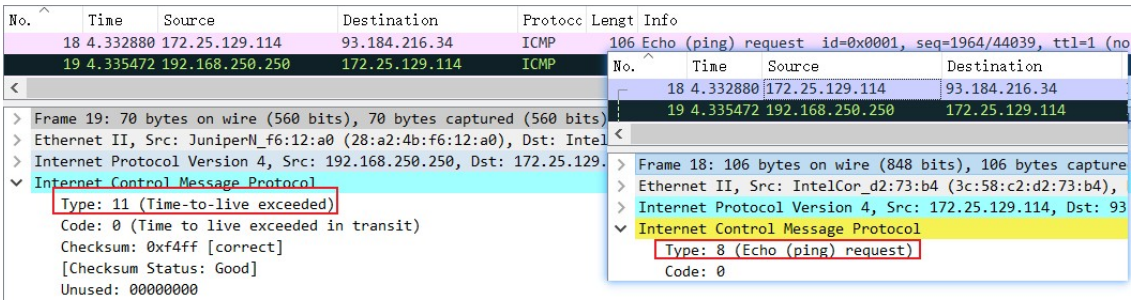
```
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x4dc5 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 1942 (0x0796)
Sequence Number (LE): 38407 (0x9607)
[Request frame: 28]
[Response time: 308.672 ms]
Data (32 bytes)
```

5. The IP address of my host is 172.25.129.114, the IP address of destination host is 93.184.216.34.

```
Source Address: 172.25.129.114
Destination Address: 93.184.216.34
```

6. No. If ICMP sent UDP packets instead, the IP protocol number should be 0x11.
7. The ICMP echo packet has the same fields as the ping query packets.
8. It contains both the IP header and the first 8 bytes of the original ICMP packet that the error is for.
9. The last three ICMP packets are message type 0 (echo reply) rather than 11 (TTL expired).

   The datagrams have made it all the way to the destination host before the TTL expired, so they are different.



10. There is a link between steps 18 and 19 that has a significantly longer delay. The header router of this link should be source host and the tail router is the destination host.