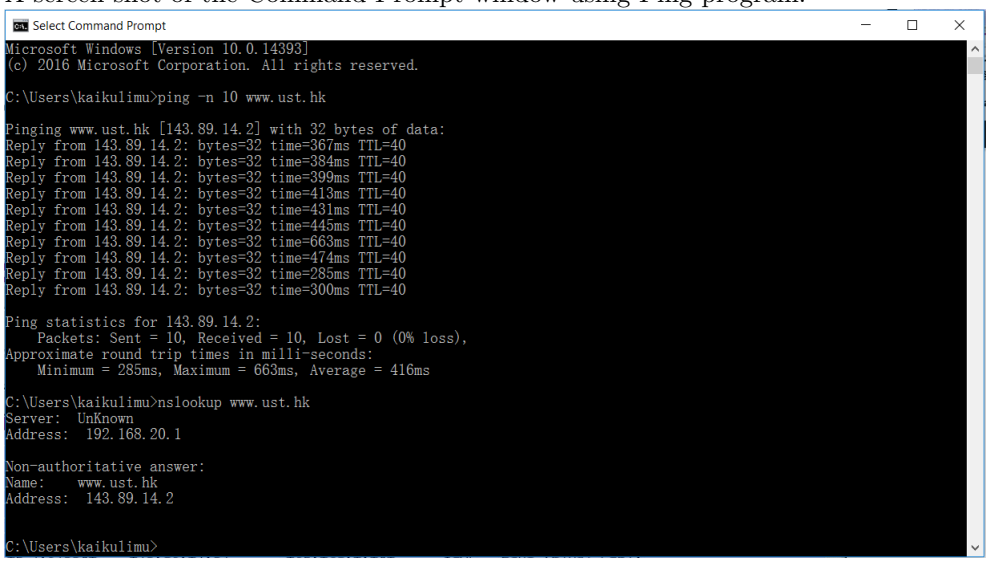
Wireshark Lab #4: ICMP

Suyi Liu, Yuan Jing Vincent Yan

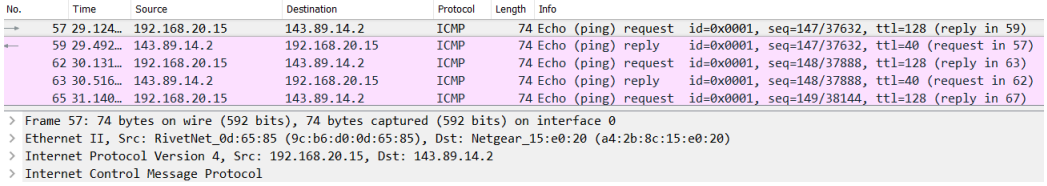
April 9, 2017

Screenshot

A screen shot of the Command Prompt window using Ping program:



Problem 1

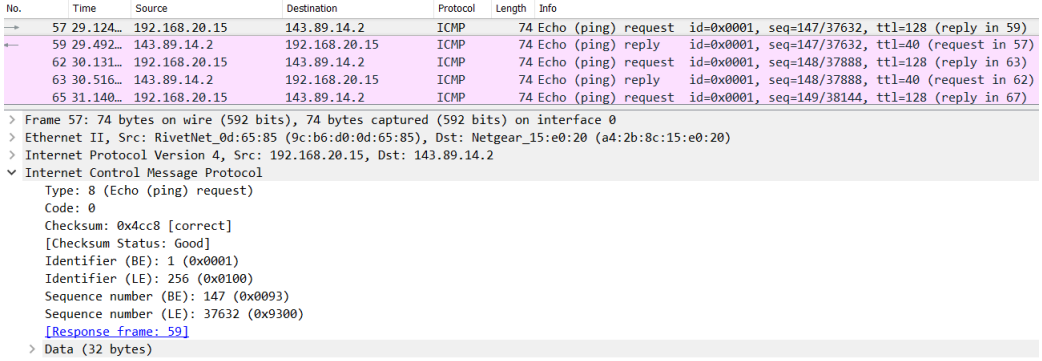


The private IP address of my host is: 192.168.20.15
(The public IP address of my host is: 71.206.30.215)
The IP address of destination host is: 143.89.14.2

Problem 2

The ICMP packet does not have source and destination port numbers because ICMP protocol is used for communication between routers and hosts, only exchanging network layer information. No port numbers are needed for upper layer application processes to communicate at this stage.

Problem 3

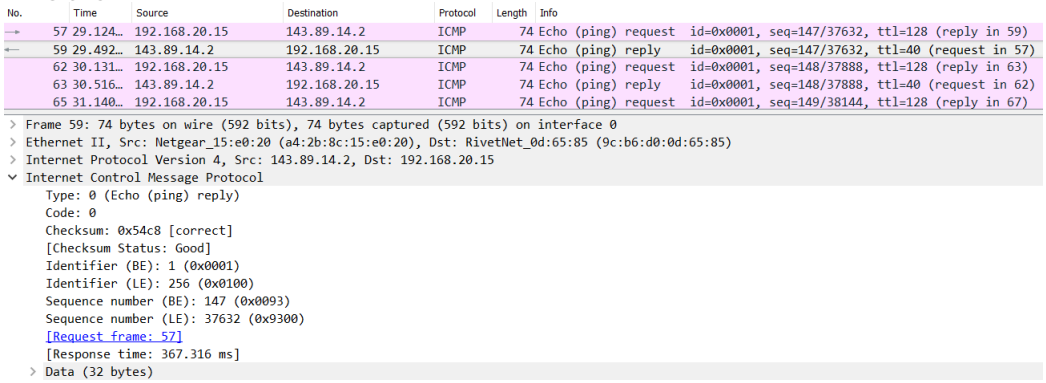


No.	Time	Source	Destination	Protocol	Length	Info
57	29.124…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (reply in 59)
59	29.492…	143.89.14.2	192.168.20.15	ICMP	74	Echo (ping) reply id=0x0001, seq=147/37632, ttl=40 (request in 57)
62	30.131…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (reply in 63)
63	30.516…	143.89.14.2	192.168.20.15	ICMP	74	Echo (ping) reply id=0x0001, seq=148/37888, ttl=40 (request in 62)
65	31.140…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=149/38144, ttl=128 (reply in 67)

```
> Frame 57: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85), Dst: Netgear_15:e0:20 (a4:2b:8c:15:e0:20)
> Internet Protocol Version 4, Src: 192.168.20.15, Dst: 143.89.14.2
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cc8 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 147 (0x0093)
    Sequence number (LE): 37632 (0x9300)
    [Response frame: 59]
  > Data (32 bytes)
```

The ICMP type is 8
The code is 0
Other fields this ICMP packet have: checksum, identifier, sequence number, and data fields
The checksum, sequence number, identifier fields are 2 bytes each.

Problem 4



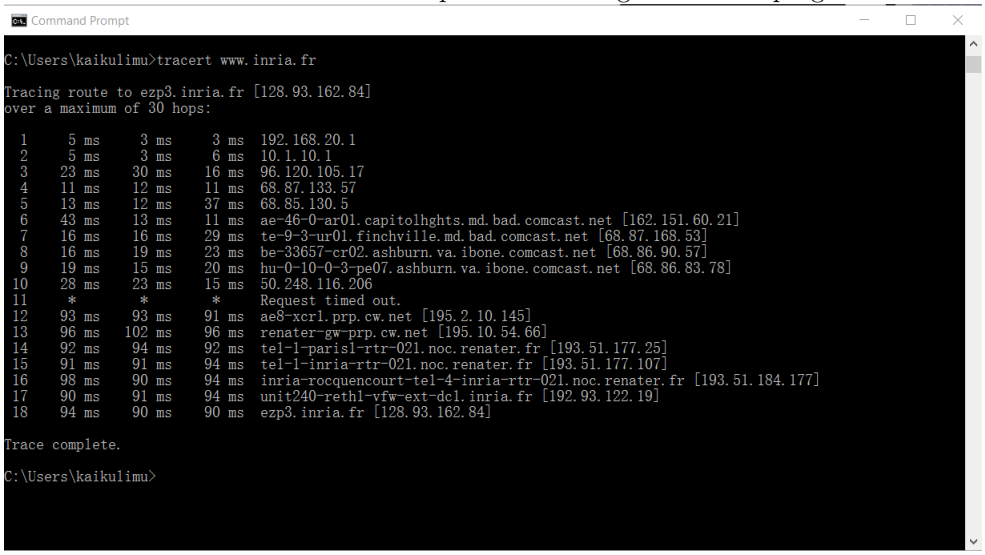
No.	Time	Source	Destination	Protocol	Length	Info
57	29.124…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (reply in 59)
59	29.492…	143.89.14.2	192.168.20.15	ICMP	74	Echo (ping) reply id=0x0001, seq=147/37632, ttl=40 (request in 57)
62	30.131…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (reply in 63)
63	30.516…	143.89.14.2	192.168.20.15	ICMP	74	Echo (ping) reply id=0x0001, seq=148/37888, ttl=40 (request in 62)
65	31.140…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=149/38144, ttl=128 (reply in 67)

```
> Frame 59: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Netgear_15:e0:20 (a4:2b:8c:15:e0:20), Dst: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85)
> Internet Protocol Version 4, Src: 143.89.14.2, Dst: 192.168.20.15
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x54c8 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 147 (0x0093)
    Sequence number (LE): 37632 (0x9300)
    [Request frame: 57]
    [Response time: 367.316 ms]
  > Data (32 bytes)
```

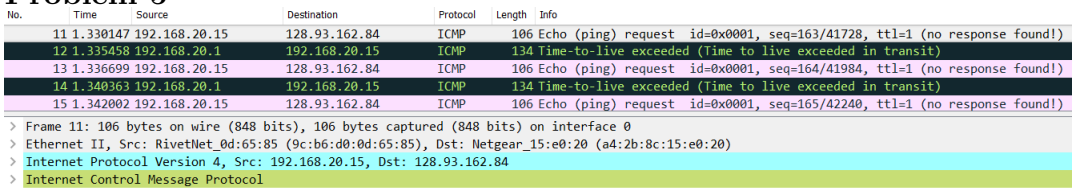
The ICMP type is 0
The code is 0
Other fields this ICMP packet have: checksum, identifier, sequence number, and data fields
The checksum, sequence number, identifier fields are 2 bytes each.

Screenshot

A screen shot of the Command Prompt window using Traceroute program:



Problem 5

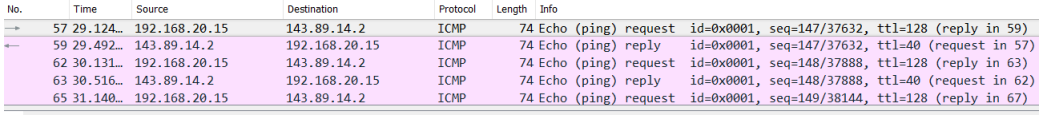


The private IP address of my host is: 192.168.20.15
(The public IP address of my host is: 71.206.30.215)
The IP address of destination host is: 128.93.162.84

Problem 6

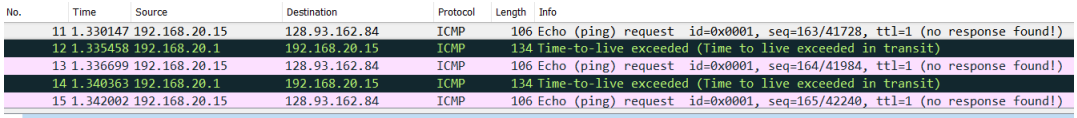
No, if ICMP sent UDP packets instead, the IP protocol number should be 0x11(17) instead.

Problem 7



No.	Time	Source	Destination	Protocol	Length	Info
57	29.124…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (reply in 59)
59	29.492…	143.89.14.2	192.168.20.15	ICMP	74	Echo (ping) reply id=0x0001, seq=147/37632, ttl=40 (request in 57)
62	30.131…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=148/37888, ttl=128 (reply in 63)
63	30.516…	143.89.14.2	192.168.20.15	ICMP	74	Echo (ping) reply id=0x0001, seq=148/37888, ttl=40 (request in 62)
65	31.140…	192.168.20.15	143.89.14.2	ICMP	74	Echo (ping) request id=0x0001, seq=149/38144, ttl=128 (reply in 67)

```
> Frame 57: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85), Dst: Netgear_15:e0:20 (a4:2b:8c:15:e0:20)
v Internet Protocol Version 4, Src: 192.168.20.15, Dst: 143.89.14.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x3ada (15066)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x8dd4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.20.15
    Destination: 143.89.14.2
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4cc8 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 147 (0x0093)
    Sequence number (LE): 37632 (0x9300)
    [Response frame: 59]
  > Data (32 bytes)
```



No.	Time	Source	Destination	Protocol	Length	Info
11	1.330147	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=163/41728, ttl=1 (no response found!)
12	1.335458	192.168.20.1	192.168.20.15	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
13	1.336699	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=164/41984, ttl=1 (no response found!)
14	1.340363	192.168.20.1	192.168.20.15	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
15	1.342002	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=165/42240, ttl=1 (no response found!)

```
> Frame 11: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85), Dst: Netgear_15:e0:20 (a4:2b:8c:15:e0:20)
v Internet Protocol Version 4, Src: 192.168.20.15, Dst: 128.93.162.84
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x6d06 (27910)
  > Flags: 0x00
    Fragment offset: 0
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x5532 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.20.15
    Destination: 128.93.162.84
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf75b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 163 (0x00a3)
    Sequence number (LE): 41728 (0xa300)
  > [No response seen]
  > Data (64 bytes)
```

As shown in the screenshots above, they are almost the same except that TTL field is different from the ICMP ping query packets in the first half of this lab. The TTL field in Ping program was 128 but the TTL field in Traceroute program is 1.

Problem 8

No.	Time	Source	Destination	Protocol	Length	Info
11	1.330147	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=163/41728, ttl=1 (no response found!)
12	1.335458	192.168.20.1	192.168.20.15	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
13	1.336699	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=164/41984, ttl=1 (no response found!)
14	1.340363	192.168.20.1	192.168.20.15	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
15	1.342002	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=165/42240, ttl=1 (no response found!)

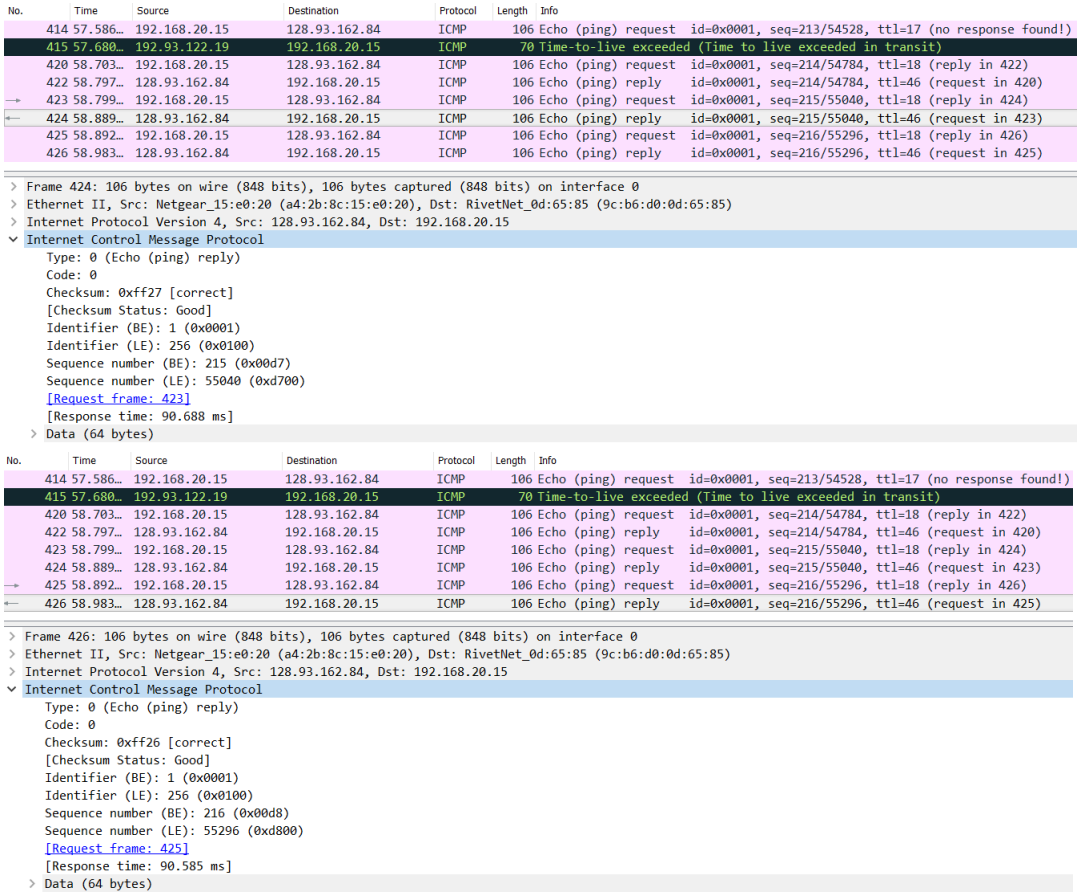
```
> Ethernet II, Src: Netgear_15:e0:20 (a4:2b:8c:15:e0:20), Dst: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85)
> Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.15
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0xf4ff [correct]
    [Checksum Status: Good]
  v Internet Protocol Version 4, Src: 192.168.20.15, Dst: 128.93.162.84
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 92
      Identification: 0x6d06 (27910)
    > Flags: 0x00
      Fragment offset: 0
    > Time to live: 1
      Protocol: ICMP (1)
      Header checksum: 0x5532 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.20.15
      Destination: 128.93.162.84
      [Source GeoIP: Unknown]
      [Destination GeoIP: Unknown]
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0xf75b [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence number (BE): 163 (0x00a3)
      Sequence number (LE): 41728 (0xa300)
    > Data (64 bytes)
```

The IP header and the first 8 bytes of the original ICMP packet are included in those fields.

Problem 9

No.	Time	Source	Destination	Protocol	Length	Info
414	57.586…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=213/54528, ttl=17 (no response found!)
415	57.680…	192.93.122.19	192.168.20.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
420	58.703…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=214/54784, ttl=18 (reply in 422)
422	58.797…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=214/54784, ttl=46 (request in 420)
423	58.799…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=215/55040, ttl=18 (reply in 424)
424	58.889…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=215/55040, ttl=46 (request in 423)
425	58.892…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=216/55296, ttl=18 (reply in 426)
426	58.983…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=216/55296, ttl=46 (request in 425)

```
> Frame 422: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Netgear_15:e0:20 (a4:2b:8c:15:e0:20), Dst: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85)
> Internet Protocol Version 4, Src: 128.93.162.84, Dst: 192.168.20.15
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff28 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 214 (0x00d6)
    Sequence number (LE): 54784 (0xd600)
    [Request frame: 420]
    [Response time: 94.069 ms]
  > Data (64 bytes)
```



No.	Time	Source	Destination	Protocol	Length	Info
414	57.586…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=213/54528, ttl=17 (no response found!)
415	57.680…	192.93.122.19	192.168.20.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
420	58.703…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=214/54784, ttl=18 (reply in 422)
422	58.797…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=214/54784, ttl=46 (request in 420)
423	58.799…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=215/55040, ttl=18 (reply in 424)
424	58.889…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=215/55040, ttl=46 (request in 423)
425	58.892…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=216/55296, ttl=18 (reply in 426)
426	58.983…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=216/55296, ttl=46 (request in 425)

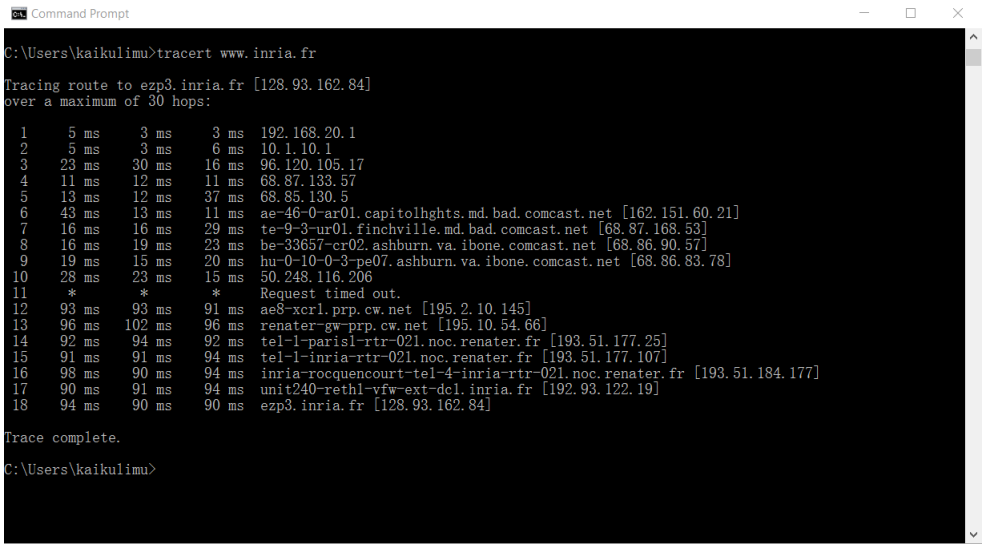
```
> Frame 424: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Netgear_15:e0:20 (a4:2b:8c:15:e0:20), Dst: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85)
> Internet Protocol Version 4, Src: 128.93.162.84, Dst: 192.168.20.15
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff27 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 215 (0x00d7)
    Sequence number (LE): 55040 (0xd700)
    [Request frame: 423]
    [Response time: 90.688 ms]
  > Data (64 bytes)
```

No.	Time	Source	Destination	Protocol	Length	Info
414	57.586…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=213/54528, ttl=17 (no response found!)
415	57.680…	192.93.122.19	192.168.20.15	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
420	58.703…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=214/54784, ttl=18 (reply in 422)
422	58.797…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=214/54784, ttl=46 (request in 420)
423	58.799…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=215/55040, ttl=18 (reply in 424)
424	58.889…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=215/55040, ttl=46 (request in 423)
425	58.892…	192.168.20.15	128.93.162.84	ICMP	106	Echo (ping) request id=0x0001, seq=216/55296, ttl=18 (reply in 426)
426	58.983…	128.93.162.84	192.168.20.15	ICMP	106	Echo (ping) reply id=0x0001, seq=216/55296, ttl=46 (request in 425)

```
> Frame 426: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
> Ethernet II, Src: Netgear_15:e0:20 (a4:2b:8c:15:e0:20), Dst: RivetNet_0d:65:85 (9c:b6:d0:0d:65:85)
> Internet Protocol Version 4, Src: 128.93.162.84, Dst: 192.168.20.15
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xff26 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 216 (0x00d8)
    Sequence number (LE): 55296 (0xd800)
    [Request frame: 425]
    [Response time: 90.585 ms]
  > Data (64 bytes)
```

As shown, these are screenshots of the last three ICMP packets received by the source host respectively.
They are type 0 messages meaning echo reply (to ping), different from 11, which indicates TTL expiration.
They are different because the datagrams have reached the destination host before the TTL has expired and the host sent the ping reply.

Problem 10



There is a link whose delay is significantly longer than others(it is either between steps 10 and 11, or between steps 11 and 12).

Referring to Figure 4, there is a link whose delay is significantly longer than others(between steps 9 and 10).

The locations of the two routers on the end of the link are not exactly known, but we guess they are somewhere in the US and somewhere in France, respectively. In Figure 4, we guess the link is from router in New York City to router in Pastourelle, France.