

1. What is the IP address of your host? What is the IP address of the destination host?

- Host IP address: 172.20.10.2
- Destination IP address: 143.89.12.134

```
gamze@MacBook-Pro ~ % ping -c 10 www.ust.hk
PING www.ust.hk (143.89.12.134): 56 data bytes
64 bytes from 143.89.12.134: icmp_seq=0 ttl=42 time=375.837 ms
64 bytes from 143.89.12.134: icmp_seq=1 ttl=42 time=393.279 ms
64 bytes from 143.89.12.134: icmp_seq=2 ttl=42 time=311.860 ms
64 bytes from 143.89.12.134: icmp_seq=3 ttl=42 time=331.139 ms
64 bytes from 143.89.12.134: icmp_seq=4 ttl=42 time=349.901 ms
64 bytes from 143.89.12.134: icmp_seq=5 ttl=42 time=471.774 ms
64 bytes from 143.89.12.134: icmp_seq=6 ttl=42 time=424.430 ms
64 bytes from 143.89.12.134: icmp_seq=7 ttl=42 time=307.957 ms
64 bytes from 143.89.12.134: icmp_seq=8 ttl=42 time=328.003 ms
64 bytes from 143.89.12.134: icmp_seq=9 ttl=42 time=328.030 ms

--- www.ust.hk ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 307.957/362.221/471.774/50.951 ms
gamze@MacBook-Pro ~ %
```

No.	Time	Source	Destination	Protocol	Length	Info
245	42.938495	172.20.10.2	172.20.16.1	ICMP	78	Destination unreachable (Port unreachable)
251	51.946100	172.20.10.2	172.20.16.1	ICMP	78	Destination unreachable (Port unreachable)
333	70.925053	172.20.10.2	143.89.12.134	ICMP	98	Echo (ping) request id=0xa804, seq=0/0, ttl=64 (reply in 334)
334	71.300659	143.89.12.134	172.20.10.2	ICMP	98	Echo (ping) reply id=0xa804, seq=0/0, ttl=42 (request in 333)
336	71.938326	172.20.10.2	143.89.12.134	ICMP	98	Echo (ping) request id=0xa804, seq=1/256, ttl=64 (reply in 337)
337	72.323388	143.89.12.134	172.20.10.2	ICMP	98	Echo (ping) reply id=0xa804, seq=1/256, ttl=42 (request in 336)
338	72.935699	172.20.10.2	143.89.12.134	ICMP	98	Echo (ping) request id=0xa804, seq=2/512, ttl=64 (reply in 339)
339	73.247207	143.89.12.134	172.20.10.2	ICMP	98	Echo (ping) reply id=0xa804, seq=2/512, ttl=42 (request in 338)
341	73.941235	172.20.10.2	143.89.12.134	ICMP	98	Echo (ping) request id=0xa804, seq=3/768, ttl=64 (reply in 342)
342	74.272855	143.89.12.134	172.20.10.2	ICMP	98	Echo (ping) reply id=0xa804, seq=3/768, ttl=42 (request in 341)
343	74.946521	172.20.10.2	143.89.12.134	ICMP	98	Echo (ping) request id=0xa804, seq=4/1024, ttl=64 (reply in 344)
344	75.296137	143.89.12.134	172.20.10.2	ICMP	98	Echo (ping) reply id=0xa804, seq=4/1024, ttl=42 (request in 343)
345	75.649125	172.20.10.2	143.89.12.134	ICMP	98	Echo (ping) request id=0xa804, seq=5/1280, ttl=64 (reply in 346)

> Frame 333: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Apple_7e:be:d0 (a4:cf:99:7e:be:d0), Dst: 2a:02:2e:b5:4f:64 (2a:02:2e:b5:4f:64)
 0100 ... Version: 4
 0101 ... Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 84
 Identification: 0xcbf4 (51444)
 000 ... Flags: 0x0
 ... 0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: ICMP (1)
 Header Checksum: 0x5fbf [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 172.20.10.2
 Destination Address: 143.89.12.134
> Internet Control Message Protocol

2. Why is it that an ICMP packet does not have source and destination port numbers?

ICMP wasn't created for use between application layer processes but instead used for exchanging network layer information between hosts and routers.

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?

```

Wi-Fi: en0
No. | Time | Source | Destination | Protocol | Length | Info
1 | 0.000000 | 172.20.10.2 | 143.89.12.134 | ICMP | 64 | 
> Frame 333: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: Apple_7e:be:d0 (a4:cf:99:7e:be:d0), Dst: 2a:02:2e:b5:4f:64 (2a:02:2e:b5:4f:64)
< Internet Protocol Version 4, Src: 172.20.10.2, Dst: 143.89.12.134
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0xc8f4 (51444)
< 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0x5fbf [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.20.10.2
Destination Address: 143.89.12.134
< Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xaaff [correct]
    [Checksum Status: Good]
    Identifier (BE): 43012 (0xa804)
    Identifier (LE): 1192 (0x4a8)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 334]
    Timestamp from icmp data: Nov 24, 2023 10:07:58.395460000 +03
    [Timestamp from icmp data (relative): 0.000127000 seconds]
> Data (48 bytes)

```

- Type: 8 (Echo (ping) request)
- Code: 0
- Other fields from this ICPM packet:
 - checksum
 - Identifiers
 - Sequence numbers
 - Data fields

Each of these data fields is two bytes.

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number, and identifier fields?

```

Wi-Fi: en0
No. | Time | Source | Destination | Protocol | Length | Info
1 | 0.000000 | 172.20.10.2 | 143.89.12.134 | ICMP | 64 | 
> Frame 334: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en0, id 0
> Ethernet II, Src: 2a:02:2e:b5:4f:64 (2a:02:2e:b5:4f:64), Dst: Apple_7e:be:d0 (a4:cf:99:7e:be:d0)
< Internet Protocol Version 4, Src: 143.89.12.134, Dst: 172.20.10.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
< Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 84
    Identification: 0x052b (1323)
< 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 42
Protocol: ICMP (1)
Header Checksum: 0x3989 [validation disabled]
[Header checksum status: Unverified]
Source Address: 143.89.12.134
Destination Address: 172.20.10.2
< Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xb2ff [correct]
    [Checksum Status: Good]
    Identifier (BE): 43012 (0xa804)
    Identifier (LE): 1192 (0x4a8)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Request frame: 333]
    [Response time: 375.606 ms]
    Timestamp from icmp data: Nov 24, 2023 10:07:58.395460000 +03
    [Timestamp from icmp data (relative): 0.375733000 seconds]
> Data (48 bytes)

```

- Type: 0 (Echo (ping) reply)
- Code: 0
- Other fields from this ICPM packet:
 - checksum
 - Identifiers
 - Sequence numbers
 - Data fields

Each of these data fields is two bytes.

5. What is the IP address of your host? What is the IP address of the target destination host?

Tracing route to inria.fr [128.93.162.83] over a maximum of 30 hops:					
1	25 ms	3 ms	2 ms	192.168.1.1	
2	9 ms	7 ms	*	10.72.0.1	
3	*	517 ms	648 ms	10.36.7.126	
4	382 ms	6 ms	6 ms	10.58.19.133	
5	29 ms	9 ms	*	10.58.19.117	
6	163 ms	15 ms	58 ms	10.58.19.126	
7	47 ms	28 ms	*	10.40.155.161	
8	21 ms	*	*	10.40.141.73	
9	665 ms	18 ms	15 ms	10.40.170.219	
10	552 ms	496 ms	642 ms	67.220.148.193	
11	528 ms	1872 ms	1084 ms	213.200.119.214	
12	915 ms	78 ms	65 ms	77.67.123.206	
13	2388 ms	59 ms	1204 ms	193.51.177.107	
14	1526 ms	730 ms	75 ms	193.51.184.177	
15	63 ms	57 ms	62 ms	192.93.122.19	
16	64 ms	99 ms	148 ms	128.93.162.83	

*Wi-Fi

DOSYA Dizende Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

icmp

No.	Time	Source	Destination	Protocol	Length	Info
289	17.055116	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=19/4864, ttl=1 (no response found!)
290	17.080481	192.168.1.1	192.168.1.24	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
291	17.083524	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=20/5120, ttl=1 (no response found!)
292	17.086364	192.168.1.1	192.168.1.24	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
293	17.089869	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=21/5376, ttl=1 (no response found!)
294	17.092249	192.168.1.1	192.168.1.24	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
333	18.102854	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=22/5632, ttl=2 (no response found!)
334	18.112149	10.72.0.1	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
335	18.115998	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=23/5888, ttl=2 (no response found!)
336	18.123013	10.72.0.1	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
337	18.126190	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=24/6144, ttl=2 (no response found!)
364	21.789814	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=25/6400, ttl=3 (no response found!)
370	25.791210	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=26/6656, ttl=3 (no response found!)
372	26.303741	10.36.7.126	192.168.1.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
386	26.308645	10.36.7.126	192.168.1.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
388	26.314056	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=27/6912, ttl=3 (no response found!)
392	26.962357	10.36.7.126	192.168.1.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
395	27.323058	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=28/7168, ttl=4 (no response found!)
404	27.784789	10.58.19.133	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
407	27.706971	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=29/7424, ttl=4 (no response found!)
408	27.713656	10.58.19.133	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
409	27.715631	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=30/7680, ttl=4 (no response found!)
410	27.721867	10.58.19.133	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
415	28.722343	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=31/7936, ttl=5 (no response found!)
417	28.761051	10.58.19.117	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
418	28.753961	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=32/8192, ttl=5 (no response found!)
419	28.762859	10.58.19.117	192.168.1.24	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
420	28.765451	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=33/8448, ttl=5 (no response found!)
488	32.293374	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=34/8704, ttl=6 (no response found!)
485	32.456648	10.58.19.126	192.168.1.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
486	32.458928	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=35/8960, ttl=6 (no response found!)
487	32.473666	10.58.19.126	192.168.1.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
488	32.477039	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=36/9216, ttl=6 (no response found!)
489	32.535013	10.58.19.126	192.168.1.24	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
508	33.486625	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=37/9472, ttl=7 (no response found!)
509	33.534676	10.40.155.161	192.168.1.24	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
510	33.536557	192.168.1.24	128.93.162.83	ICMP	106	Echo (ping) request id=0x0001, seq=38/9728, ttl=7 (no response found!)
511	33.564698	10.40.155.161	192.168.1.24	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)

```

No.      Time           Source          Destination        Protocol Length Info
293 17.089869 192.168.1.24 128.93.162.83 ICMP    106 Echo (ping) request id=0x0001, seq=21/5376, ttl=1 (no
response found!)
Frame 293: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{91D046C6-D7DA-47BD-A238-95655C493B71}, id 0
Ethernet II, Src: IntelCor_44:ac:c8 (c8:b2:9b:44:ac:c8), Dst: HuaweiTe_87:da:4f (f0:c8:50:87:da:4f)
Internet Protocol Version 4, Src: 192.168.1.24, Dst: 128.93.162.83
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    ... .00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 92
    Identification: 0xc995 (51605)
    000.... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 1
    [Expert Info (Note/Sequence): "Time To Live" only]
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.24
    Destination Address: 128.93.162.83
    Internet Control Message Protocol

```

Source

192.168.1.24

Destination

128.93.162.83

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol number still be 01 for the probe packets? If not, what would it be?

No, it won't be 01 for the probe packets. It would be 0x11. This is because the protocol number in the IP header needs to accurately reflect the protocol used in the payload of the IP packet.

7. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP ping packet. What is included in those fields?

They both have the IP header and the first 8 bytes from the original ICMP packet that caused the error.

```
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport
Total Length: 92
Identification: 0xc995 (51605)
v 000. .... = Flags: 0x0
    0.... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...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: 0x0b9b [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.24
Destination Address: 128.93.162.83
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xf7e9 [unverified] [in ICMP error packet]
    [Checksum Status: Unverified]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 21 (0x0015)
    Sequence Number (LE): 5376 (0x1500)
    > Data (64 bytes)
```

8. Within the traceroute measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in your figure, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two routers on the end of this link?

In my screenshot, we can see, specifically, notice the high round-trip times (RTTs) at hops 3, 4, 9, 10, 11, 12, and 13. The link is from New York to France.

```
Tracing route to inria.fr [128.93.162.83]
over a maximum of 30 hops:

 1  25 ms      3 ms      2 ms  192.168.1.1
 2  9 ms       7 ms      *     10.72.0.1
 3  *          517 ms    648 ms  10.36.7.126
 4  382 ms     6 ms      6 ms  10.58.19.133
 5  29 ms      9 ms      *     10.58.19.117
 6  163 ms     15 ms     58 ms  10.58.19.126
 7  47 ms      28 ms      *     10.40.155.161
 8  21 ms      *          *     10.40.141.73
 9  665 ms     18 ms     15 ms  10.40.170.219
10  552 ms     496 ms    642 ms  67.220.148.193
11  528 ms     1872 ms   1084 ms  213.200.119.214
12  915 ms     78 ms     65 ms  77.67.123.206
13  2388 ms    59 ms    1204 ms  193.51.177.107
14  1526 ms    730 ms    75 ms  193.51.184.177
15  63 ms      57 ms     62 ms  192.93.122.19
16  64 ms      99 ms    148 ms  128.93.162.83

Trace complete.
```