

HACETTEPE UNIVERSITY  
COMPUTER ENGINEERING DEPARTMENT  
BBM 453 LAB EXPERIMENT 6 (ICMP)



Group No: 41  
Yiğit Emir Işıkcı: 2200356028  
Ahmet Eren Akbaş: 21945757

# 1) Introduction to ICMP Wireshark Lab

The Internet Control Message Protocol, or ICMP for short, is super important for keeping computer networks running smoothly. It helps figure out if there are any issues with the connection and how data gets from one computer to another. In this Wireshark Lab about ICMP, we get to really see how ICMP works by doing some hands-on activities.

We're going to look closely at messages that come from two important tools we use in networks: Ping and Traceroute. Ping is a tool that helps us see if another computer on the network can be reached and how long it takes to get a message to it and back. If any messages get lost on the way, Ping will tell us. Traceroute is another tool that shows us the path messages take to reach another computer and helps us see where delays happen.

## 2) Part 1: Ping

```
C:\Windows\System32>ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.12.134] with 32 bytes of data:
Reply from 143.89.12.134: bytes=32 time=255ms TTL=48
Reply from 143.89.12.134: bytes=32 time=324ms TTL=48
Reply from 143.89.12.134: bytes=32 time=254ms TTL=48
Reply from 143.89.12.134: bytes=32 time=254ms TTL=48
Reply from 143.89.12.134: bytes=32 time=272ms TTL=48
Reply from 143.89.12.134: bytes=32 time=289ms TTL=48
Reply from 143.89.12.134: bytes=32 time=254ms TTL=48
Reply from 143.89.12.134: bytes=32 time=314ms TTL=48
Reply from 143.89.12.134: bytes=32 time=326ms TTL=48
Reply from 143.89.12.134: bytes=32 time=341ms TTL=48

Ping statistics for 143.89.12.134:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 254ms, Maximum = 341ms, Average = 288ms
```

- The Ping program successfully reached the host www.ust.hk with the IP address 143.89.12.134, indicating that the host is live and responding.
- The round-trip times (RTT) fluctuated between 254ms and 341ms. This variability in RTT could be due to network congestion, routing paths changes, or the load on the host server.
- All ten ICMP packets sent received a reply, which shows there was no packet loss during this particular ping session.

### 2.1) What is the IP address of your host? What is the IP address of the destination host?

The image shows a Wireshark packet capture of ICMP Echo (ping) traffic. The top pane lists 20 packets, alternating between requests and replies. The middle pane shows the details of the selected packet (No. 11), identifying it as an Internet Protocol Version 4 packet with source 10.225.144.231 and destination 143.89.12.134. The bottom pane shows the raw packet bytes in hexadecimal and ASCII.

The IP address of my host, from which the ping was initiated, is 10.225.144.231. This can be seen as the source address in the IP header for the echo request packets.

The IP address of the destination host, to which the ping was sent, is 143.89.12.134. This is shown as the destination address in the IP header for the echo request packets.

## 2.2) Why is it that an ICMP packet does not have source and destination port numbers?

An ICMP packet does not have source and destination port numbers because it is not designed to carry application-level data, which is what ports are generally used for.

Instead, ICMP is used for sending error messages and operational information pertaining to IP operations. Port numbers are associated with the Transport layer protocols like TCP and UDP, which facilitate application data transfer.

ICMP operates at the network layer and serves different purposes, such as diagnosing network communication issues or reporting about unreachable hosts or networks. This distinction is why ICMP packets are structured without port numbers, unlike TCP or UDP packets.

## 2.3) 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?

No.	Time	Source	Destination	Protocol	Length	Info
6	3.790289	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 8)
8	4.045521	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=48 (request in 6)
15	4.797303	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 16)
16	5.121998	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=48 (request in 15)
17	5.805990	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 24)
24	6.060448	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=48 (request in 17)
28	6.814134	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 35)
35	7.068043	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=48 (request in 28)
36	7.820404	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 40)
40	8.092354	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=48 (request in 36)
45	8.826825	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 46)
46	9.116084	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=48 (request in 45)
55	9.845397	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 57)
57	10.099525	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=48 (request in 55)
59	10.849900	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 60)
60	11.164006	143.89.12.134	10.225.144.231	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=48 (request in 59)
61	11.861746	10.225.144.231	143.89.12.134	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 62)

> Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{780BF...}	0000 02 e0 52 0a 97 e1 90 e8 68 2c 61 c7 08 00 45 00	--R----- h,a---E-
> Ethernet II, Src: AzureWav_2c:61:c7 (90:e8:68:2c:61:c7), Dst: 02:e0:52:0a:97:e1 (02:e0:52:0a:97:e1)	0010 00 3c a0 23 00 00 80 01 62 f6 0a e1 90 e7 8f 59	<-#---- b,---Y
> Internet Protocol Version 4, Src: 10.225.144.231, Dst: 143.89.12.134	0020 0c 86 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66	....MZ... ..abcdef
> Internet Control Message Protocol	0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv
Type: 8 (Echo (ping) request)	0040 77 61 62 63 64 65 66 67 68 69	wabcdefg hi
Code: 0		
Checksum: 0x4d5a [correct]		
[Checksum Status: Good]		
Identifier (BE): 1 (0x0001)		
Identifier (LE): 256 (0x0100)		
Sequence Number (BE): 1 (0x0001)		
Sequence Number (LE): 256 (0x0100)		
[Response frame: 8]		
> Data (32 bytes)		

The ICMP type is 8, which indicates an echo (ping) request. The code for this type of ICMP packet is 0, which is standard for echo requests.

#### Other Fields:

- The Checksum is 0x4d5a, which indicates that the packet is valid and is 2 bytes long
- The Identifier (BE) is 0x0001 and in Little-Endian (LE) is 256 (0x0100). This identifier helps in matching echo requests with their corresponding replies. This field is also 2 bytes long.
- The Sequence Number (BE) is 0x0001 and in LE is 256 (0x0100). This number increments with each new echo request sent. This field is also 2 bytes long as we can see from the hexadecimal format.

## 2.4) 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?

The screenshot shows a Wireshark packet capture of ICMP Echo (ping) traffic. The packet list at the top shows a sequence of requests and replies. The selected packet is Frame 8, an ICMP Echo (ping) reply from 143.89.12.134 to 10.225.144.231. The packet details pane on the right shows the following fields:

- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x555a [correct]
- [Checksum Status: Good]
- Identifier (BE): 1 (0x0001)
- Identifier (LE): 256 (0x0100)
- Sequence Number (BE): 1 (0x0001)
- Sequence Number (LE): 256 (0x0100)
- [Request frame: 6]
- [Response time: 255,232 ms]

The packet data (32 bytes) is shown in the bottom pane, displaying the raw bytes of the ICMP echo reply.

The ICMP type for the reply is 0, which indicates an echo reply, and the code is 0. This is typical for ICMP echo replies, confirming that the destination has received the echo request and is responding back.

### Other Fields:

- The Checksum for this packet is 0x555a, and it is marked as correct, indicating no corruption in the packet data during transit.
- The Identifier (BE) is 0x0001 and in Little-Endian (LE) is 256 (0x0100). This matches the identifier in the echo request, confirming that this reply corresponds to the initial request.
- The Sequence Number (BE) is 0x0001 and in LE is 256 (0x0100). This, too, matches the sequence number in the request, helping to match each reply to its corresponding request.

The bytes of these fields are 2, same as the request packet.

## 3) Part 2: Traceroute

```

C:\Windows\System32>tracert gaia.cs.umass.edu

Tracing route to gaia.cs.umass.edu [128.119.245.12]
over a maximum of 30 hops:

  1  *          2 ms      <1 ms    10.225.255.3
  2  5 ms       3 ms       3 ms     192.168.200.252
  3  2 ms       3 ms       2 ms     192.168.216.240
  4  *          *          *          Request timed out.
  5  8 ms       8 ms       9 ms     193.140.0.150
  6  *          29 ms      31 ms    ulakbim.mx1.bud.hu.geant.net [62.40.125.129]
  7  56 ms      56 ms      74 ms    ae9.mx1.vie.at.geant.net [62.40.98.45]
  8  57 ms      56 ms      56 ms    ae5.rt1.pra.cz.geant.net [62.40.98.242]
  9  99 ms      44 ms      44 ms    ae6.rt1.fra.de.geant.net [62.40.98.158]
 10  55 ms      55 ms      56 ms    ae3.mx1.lon.uk.geant.net [62.40.98.179]
 11  144 ms     164 ms     141 ms    internet2-gw.mx1.lon.uk.geant.net [62.40.124.45]
 12  170 ms     237 ms     141 ms    fourhundredge-0-0-0-0.4079.core1.ashb.net.internet2.edu [163.253.1.118]
 13  149 ms     156 ms     142 ms    fourhundredge-0-0-0-1.4079.core1.newy32aoa.net.internet2.edu [163.253.1.117]
 14  140 ms     153 ms     141 ms    fourhundredge-0-0-0-20.4079.core2.newy32aoa.net.internet2.edu [163.253.1.43]
 15  144 ms     177 ms     144 ms    nox300gw1-12-re.nox.org [192.5.89.221]
 16  146 ms     167 ms     153 ms    192.5.89.58
 17  148 ms     150 ms     146 ms    nox-mghpcc-gw1-umassnet-re2.nox.org [18.2.8.90]
 18  173 ms     236 ms     147 ms    69.16.1.0
 19  175 ms     146 ms     146 ms    core1-rt-et-8-3-0.gw.umass.edu [192.80.83.109]
 20  148 ms     151 ms     146 ms    n1-rt-1-1-et-0-0-0.gw.umass.edu [128.119.0.216]
 21  147 ms     234 ms     147 ms    128.119.7.74
 22  *          147 ms     150 ms    128.119.7.66
 23  148 ms     168 ms     147 ms    core1-rt-et-7-2-1.gw.umass.edu [128.119.0.217]
 24  147 ms     168 ms     149 ms    n5-rt-1-1-xe-2-1-0.gw.umass.edu [128.119.3.33]
 25  147 ms     260 ms     151 ms    cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
 26  149 ms     266 ms     148 ms    nscs1bbs1.cs.umass.edu [128.119.240.253]
 27  148 ms     147 ms     147 ms    gaia.cs.umass.edu [128.119.245.12]

Trace complete.

```

### 3.1) What is the IP address of your host? What is the IP address of the target destination host?

The screenshot shows a Wireshark capture of ICMP echo (ping) requests. The packet list on the left shows several failed requests with 'Time to live exceeded' or 'Destination unreachable' messages. The packet details pane on the right shows the IP header for the selected packet, with the Source Address: 10.225.144.231 and Destination Address: 128.119.245.12 highlighted in red.

No.	Time	Source	Destination	Protocol	Length	Info
6	1.134268	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=11/2816, ttl=1 (no response found!)
12	5.071923	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=12/3072, ttl=1 (no response found!)
13	5.074846	10.225.255.3	10.225.144.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	5.075083	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=1 (no response found!)
15	5.075826	10.225.255.3	10.225.144.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	5.497573	10.225.255.3	10.225.144.231	ICMP	70	Destination unreachable (Port unreachable)
27	7.023947	10.225.255.3	10.225.144.231	ICMP	70	Destination unreachable (Port unreachable)
29	8.508680	10.225.255.3	10.225.144.231	ICMP	70	Destination unreachable (Port unreachable)
40	11.036270	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=14/3584, ttl=2 (no response found!)
41	11.041232	192.168.200.252	10.225.144.231	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
42	11.042287	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=15/3840, ttl=2 (no response found!)
43	11.045715	192.168.200.252	10.225.144.231	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
44	11.046780	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=2 (no response found!)
45	11.050602	192.168.200.252	10.225.144.231	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
52	17.000729	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=17/4352, ttl=3 (no response found!)
53	17.003389	192.168.216.240	10.225.144.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54	17.004142	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=18/4608, ttl=3 (no response found!)

Frame 6: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface Device\NPF\_{7...}

Ethernet II, Src: AzureWav\_2c:61:c7 (90:e8:68:2c:61:c7), Dst: 02:e0:52:0a:97:e1 (02:e0:52:0a:97:..)

Internet Protocol Version 4, Src: 10.225.144.231, Dst: 128.119.245.12

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 92

Identification: 0xfdbb (64955)

000. .... = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 1

Protocol: ICMP (1)

Header Checksum: 0xaa99 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.225.144.231

Destination Address: 128.119.245.12

The IP address of my host, from which the ICMP packets are being sent, is 10.225.144.231. This is visible in the 'Source Address' field of the IP header for the ICMP echo (ping) request highlighted in the screenshot.

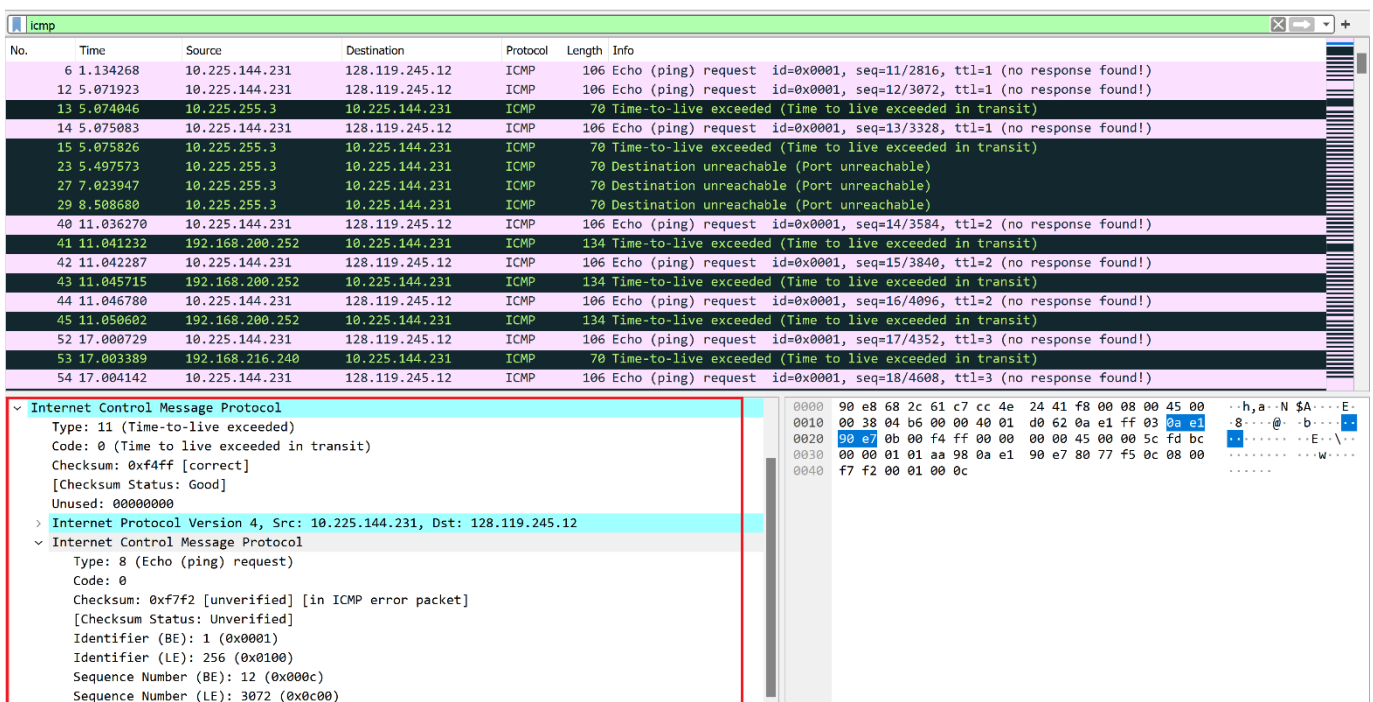


The IP address of the target destination host, to which the ICMP packets are being sent, is 128.119.245.12. Which is the ip address of the hostname “gaia.cs.umass.edu”.

### 3.2) 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, the IP protocol number would not be 01 if ICMP used UDP packets for the probes. The protocol number for ICMP is 01, but for UDP, it is 17.

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



No.	Time	Source	Destination	Protocol	Length	Info
6	1.134268	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=11/2816, ttl=1 (no response found!)
12	5.071923	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=12/3072, ttl=1 (no response found!)
13	5.074046	10.225.255.3	10.225.144.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
14	5.075083	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=13/3328, ttl=1 (no response found!)
15	5.075826	10.225.255.3	10.225.144.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
23	5.497573	10.225.255.3	10.225.144.231	ICMP	70	Destination unreachable (Port unreachable)
27	7.023947	10.225.255.3	10.225.144.231	ICMP	70	Destination unreachable (Port unreachable)
29	8.508680	10.225.255.3	10.225.144.231	ICMP	70	Destination unreachable (Port unreachable)
40	11.036270	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=14/3584, ttl=2 (no response found!)
41	11.041232	192.168.200.252	10.225.144.231	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
42	11.042287	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=15/3840, ttl=2 (no response found!)
43	11.045715	192.168.200.252	10.225.144.231	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
44	11.046780	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=16/4096, ttl=2 (no response found!)
45	11.050602	192.168.200.252	10.225.144.231	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
52	17.000729	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=17/4352, ttl=3 (no response found!)
53	17.003389	192.168.216.240	10.225.144.231	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
54	17.004142	10.225.144.231	128.119.245.12	ICMP	106	Echo (ping) request id=0x0001, seq=18/4608, ttl=3 (no response found!)

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
Internet Protocol Version 4, Src: 10.225.144.231, Dst: 128.119.245.12	
Internet Control Message Protocol	
Type: 8 (Echo (ping) request)	
Code:	0
Checksum:	0xf7f2 [unverified] [in ICMP error packet]
[Checksum Status:	Unverified]
Identifier (BE):	1 (0x0001)
Identifier (LE):	256 (0x0100)
Sequence Number (BE):	12 (0x000c)
Sequence Number (LE):	3072 (0xc000)

Offset	Hex	ASCII
0000	90 e8 68 2c 61 c7 cc 4e 24 41 f8 00 08 00 45 00	..h,a..N \$A...E..
0010	00 38 04 b6 00 00 40 01 d0 62 0a e1 ff 03 0a e1	..8...@..b...E..
0020	00 e7 0b 00 f4 ff 00 00 00 00 45 00 00 5c fd bc	..E...w... ..
0030	00 00 01 01 aa 98 0a e1 90 e7 80 77 f5 0c 08 00	.....w... ..
0040	f7 f2 00 01 00 0c	.....

The ICMP error packet includes the original IP header and the first 8 bytes of the ICMP payload that triggered the error.

It includes original IP header because it provides context for the error message, indicating the source and destination IP addresses of the packet that encountered the error. This is

crucial for the sender to understand which packet was affected and to which destination it was headed.

It includes first 8 bytes of the ICMP payload because these bytes help to uniquely identify the original ICMP request that triggered the error message.

**3.4) 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?**

```
C:\Windows\System32>tracert gaia.cs.umass.edu

Tracing route to gaia.cs.umass.edu [128.119.245.12]
over a maximum of 30 hops:

  0  *          2 ms    <1 ms   10.225.255.3
  1  5 ms       3 ms     3 ms   192.168.200.252
  2  2 ms       3 ms     2 ms   192.168.216.240
  3  *          *        *        Request timed out.
  4  8 ms       8 ms     9 ms   193.140.0.150
  5  *          29 ms    31 ms   ulakbim.mx1.bud.hu.geant.net [62.40.125.129]
  6  56 ms      56 ms    74 ms   ae9.mx1.vie.at.geant.net [62.40.98.45]
  7  57 ms      56 ms    56 ms   ae5.rtl.pra.cz.geant.net [62.40.98.242]
  8  99 ms      44 ms    44 ms   ae6.rtl.fra.de.geant.net [62.40.98.158]
  9  55 ms      55 ms    56 ms   ae3.mx1.lon.uk.geant.net [62.40.98.179]
 10 144 ms     164 ms   141 ms   internet2-gw.mx1.lon.uk.geant.net [62.40.124.45]
 11 170 ms     237 ms   141 ms   fourhundredge-0-0-0-0.4079.core1.ashb.net.internet2.edu [163.253.1.118]
 12 149 ms     156 ms   142 ms   fourhundredge-0-0-0-1.4079.core1.newy32aoa.net.internet2.edu [163.253.1.117]
 13 140 ms     153 ms   141 ms   fourhundredge-0-0-0-20.4079.core2.newy32aoa.net.internet2.edu [163.253.1.43]
 14 144 ms     177 ms   144 ms   nox300gw1-i2-re.nox.org [192.5.89.221]
 15 146 ms     167 ms   153 ms   192.5.89.58
 16 148 ms     150 ms   146 ms   nox-mghpcc-gw1-umassnet-re2.nox.org [18.2.8.90]
 17 173 ms     236 ms   147 ms   69.16.1.0
 18 175 ms     146 ms   146 ms   core1-rt-et-8-3-0.gw.umass.edu [192.80.83.109]
 19 148 ms     151 ms   146 ms   n1-rt-1-1-et-0-0-0.gw.umass.edu [128.119.0.216]
 20 147 ms     234 ms   147 ms   128.119.7.74
 21 *          147 ms   150 ms   128.119.7.66
 22 148 ms     168 ms   147 ms   core1-rt-et-7-2-1.gw.umass.edu [128.119.0.217]
 23 147 ms     168 ms   149 ms   n5-rt-1-1-xe-2-1-0.gw.umass.edu [128.119.3.33]
 24 147 ms     260 ms   151 ms   cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
 25 149 ms     266 ms   148 ms   nscs1bbs1.cs.umass.edu [128.119.240.253]
 26 148 ms     147 ms   147 ms   gaia.cs.umass.edu [128.119.245.12]
```

The link between 10th and 11th hop has a significantly longer delay. But we could not guess the locations of these routers. It is not written explicitly.