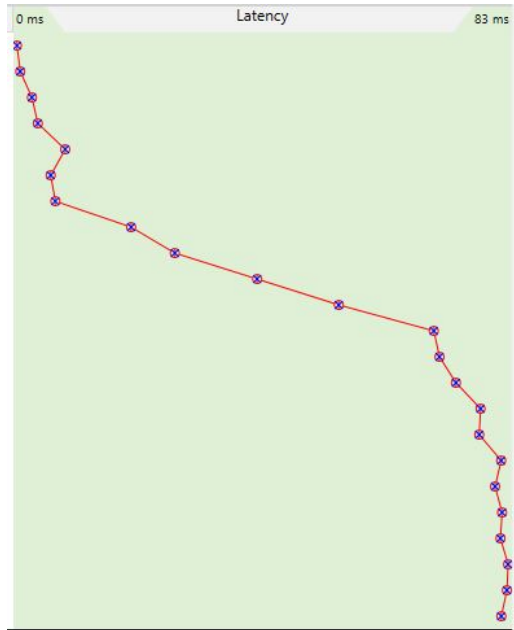


Using the 56-byte packet-size ping capture data

1. Provide a screenshot of pingplotter tracing graph for 56-byte packet size.



2. In Wireshark, select the first ICMP Echo Request message sent by your computer and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer? Provide relevant screenshot to illustrate and support your answer.

The IP address of my computer is 192.168.50.31.

1	0.000000	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=630/30210, ttl=255 (reply in 4)
2	0.000437	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=631/30466, ttl=4 (no response found!)
3	0.050712	192.168.50.1	192.168.50.31	ICMP	90 time-to-live exceeded (Time to live exceeded in transit)	
4	0.081528	128.119.245.12	192.168.50.31	ICMP	70 Echo (ping) reply	id=0x0001, seq=630/30210, ttl=43 (request in 1)
5	0.100913	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=632/30722, ttl=2 (no response found!)
6	0.101849	192.168.1.254	192.168.50.31	ICMP	98 time-to-live exceeded (Time to live exceeded in transit)	
7	0.113116	192.168.50.31	192.168.50.1	DNS	85 Standard query 0x37cf PTR 1.50.168.192.in-addr.arpa	
8	0.113697	192.168.50.1	192.168.50.31	DNS	114 Standard query response 0x37cf PTR 1.50.168.192.in-addr.arpa PTR router.asus.com	
9	0.115744	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=633/30978, ttl=3 (no response found!)
10	0.115756	192.168.50.31	192.168.50.1	DNS	86 Standard query 0x3d88 PTR 254.1.168.192.in-addr.arpa	
11	0.115453	100.206.148.1	192.168.50.31	ICMP	90 time-to-live exceeded (Time to live exceeded in transit)	
12	0.1154714	192.168.50.1	192.168.50.31	DNS	122 Standard query response 0x3d88 PTR 254.1.168.192.in-addr.arpa PTR dsdevice.attlocal.net	
13	0.202518	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=634/31234, ttl=4 (no response found!)
14	0.202519	25.78.109.104	192.168.50.31	ICMP	90 time-to-live exceeded (Time to live exceeded in transit)	
15	0.253104	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=635/31490, ttl=5 (no response found!)
16	0.253874	192.168.50.31	192.168.50.1	DNS	85 Standard query 0x8248 PTR 104.48.29.75.in-addr.arpa	
17	0.261501	12.242.115.3	192.168.50.31	ICMP	110 time-to-live exceeded (Time to live exceeded in transit)	
18	0.288872	192.168.50.31	192.168.50.1	DNS	85 Standard query 0x8248 PTR 104.48.29.75.in-addr.arpa	
19	0.303481	192.108.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=636/31740, ttl=6 (no response found!)
20	0.309453	154.54.13.160	192.168.50.31	ICMP	110 time-to-live exceeded (Time to live exceeded in transit)	
21	0.314719	192.168.50.31	192.168.50.1	DNS	85 Standard query 0x1469 PTR 3.115.242.12.in-addr.arpa	
22	0.322605	192.168.50.1	192.168.50.31	DNS	172 Standard query response 0x1469 No such name PTR 3.115.242.12.in-addr.arpa SOA xbru.br.ns.els.gms.att.net	
23	0.322984	192.168.50.31	12.242.115.3	HNS	92 Name query HBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00>	
24	0.353825	192.168.50.31	128.119.245.12	ICMP	70 Echo (ping) request	id=0x0001, seq=637/32002, ttl=7 (no response found!)

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{58786FDC-B88D-4E84-A301-1455E3F21450}, id 0

Ethernet II, Src: Universa_28:cb:92 (00:21:86:28:cb:92), Dst: ASUSTek_01:40:f4 (88:d7:f6:01:40:f4)

Internet Protocol Version 4, Src: 192.168.50.31, 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: 56

Identification: 0x362c (13868)

Flags: 0x00

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

Time to Live: 255

Protocol: ICMP (1)

Header Checksum: 0x0000 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.50.31

Destination Address: 128.119.245.12

Internet Control Message Protocol

3. Within the IP packet header, what is the value in the upper layer protocol field? Provide screenshot(s) to illustrate and support your answer.

ICMP (1)

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
    Identification: 0x362c (13868)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.31
    Destination Address: 128.119.245.12
```

4. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes. Provide screenshot(s) to illustrate and support your answer.

The IP header 20 bytes. Payload header bytes is the total length minus the IP header bytes which is 56-20 which is 36 bytes.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
    Identification: 0x362c (13868)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.31
    Destination Address: 128.119.245.12
```

5. Has this IP datagram been fragmented? Explain how you determined whether the datagram has been fragmented. Provide screenshot(s) to illustrate and support your answer.

The IP datagram has not been fragmented because the more fragments bit = 0 so the data is not fragmented.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
    Identification: 0x362c (13868)
  > Flags: 0x00
    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: 255
    Protocol: ICMP (1)
```

6. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer? Provide screenshot(s) to illustrate and support your answer.

The identification field and the time to live is always changing.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
Identification: 0x3645 (13893)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 25
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12
```

7. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why? Provide screenshot(s) to illustrate and support your answer.

The fields that stay constant and must stay constant are version since we are using version IPv4, header length since we are using IPv4, source IP since my computers IP doesn't change, destination IP since we are sending to the same host, differentiated services since we are sending to the same protocol every time, upper layer protocol since it is the same protocol every time, header checksum since validation is disabled.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
Identification: 0x3645 (13893)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 25
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12
```

The fields that must change are the Identification field since each IP datagram has a different ID and the time to live since that is how trace routing works.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
Identification: 0x3645 (13893)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 25
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12
```

8. Describe the pattern you see in the values in the Identification field of the IP datagram. Provide screenshot(s) to illustrate and support your answer.

The identification field is only incrementing by one at every request for example the first request is 13892 the second request is 13893.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
    Identification: 0x3645 (13893)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 25
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.31
    Destination Address: 128.119.245.12
```

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 56
    Identification: 0x3644 (13892)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 24
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.31
    Destination Address: 128.119.245.12
```

9. What is the value in the Identification field and the TTL field? Provide screenshot(s) to illustrate and support your answer.

The Identification value is 0 and the time to live value is 239.

```
Internet Protocol Version 4, Src: 69.16.1.0, Dst: 192.168.50.31
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 239
    Protocol: ICMP (1)
    Header Checksum: 0x92ed [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 69.16.1.0
    Destination Address: 192.168.50.31
```

10. Do these values remain unchanged for all the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why? Provide screenshot(s) to illustrate and support your answer.

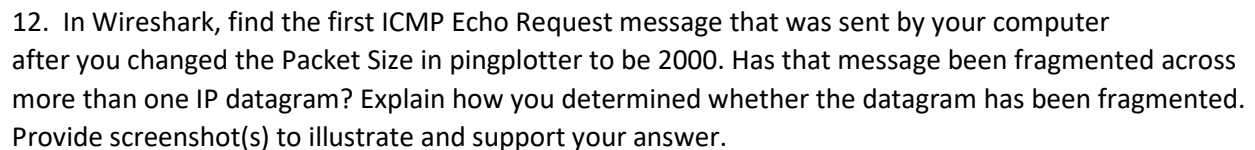
The values of the identification field for all the ICMP TTL-exceeded replies do change since the identification field is a unique value. If two or more IP datagrams have the same identification value its because those IP datagrams are fragments to one large IP datagram.

```
Internet Protocol Version 4, Src: 75.29.48.104, Dst: 192.168.50.31
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x5312 (21266)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 61
    Protocol: ICMP (1)
    Header Checksum: 0xbc22 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 75.29.48.104
    Destination Address: 192.168.50.31
```

```
Internet Protocol Version 4, Src: 69.16.1.0, Dst: 192.168.50.31
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 239
    Protocol: ICMP (1)
    Header Checksum: 0x92ed [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 69.16.1.0
    Destination Address: 192.168.50.31
```

```
Internet Protocol Version 4, Src: 69.16.0.8, Dst: 192.168.50.31
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x0000 (0)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 239
    Protocol: ICMP (1)
    Header Checksum: 0x93e5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 69.16.0.8
    Destination Address: 192.168.50.31
```

11. Provide a screenshot of pingplotter tracing graph for 2000-byte packet size.

[illegible]

13. From the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram? Provide screenshot(s) to illustrate and support your answer.

I turned off the Resembled fragment IPv4 Datagrams for this. In the Flags it shows a bit is set indicating the datagram has been fragmented and there are more fragments. And the fragment offset is zero meaning it is the first fragment. The IP datagram is 1500 bytes.

14. From the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell? Provide screenshot(s) to illustrate and support your answer.

From the fragmented IP datagram, the fragment offset is 1480 meaning it is the total offset. The reason we know this is the total is because there are no more fragments as well according to the more fragments bit not being set.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 520
    Identification: 0x397e (14718)
  < Flags: 0x00
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0101 1100 1000 = Fragment Offset: 1480
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.31
    Destination Address: 128.119.245.12
```

15. What fields change in the IP header between the first and second fragment? Provide screenshot(s) to illustrate and support your answer.

The total length, the more fragments bit, and fragment offset.

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 1500
    Identification: 0x397e (14718)
  < Flags: 0x20, More fragments
    0... .... = Reserved bit: Not set
    .0... .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 255
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.50.31
    Destination Address: 128.119.245.12
```

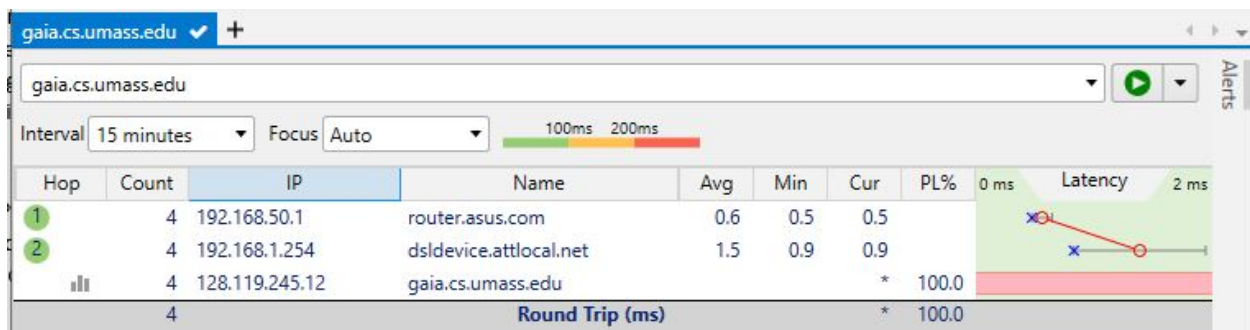
```

Internet Protocol Version 4, Src: 192.168.50.31, 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: 520
Identification: 0x397e (14718)
▼ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12

```

Using the 3500-byte packet-size ping capture data

16. Provide a screenshot of pingplotter tracing graph for 3500-byte packet size.



17. In Wireshark, how many fragments were created from the original datagram? Provide screenshot(s) to illustrate and support your answer.

There were 3 packets created from the original datagram.

2	0.273528	192.168.50.31	128.119.245.12	ICMP	15...	Echo (ping) request id=0x0001, seq=2082/8712, ttl=255 (no response found!)
3	0.273528	192.168.50.31	128.119.245.12	IPv4	15...	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=3aa2)
4	0.273528	192.168.50.31	128.119.245.12	IPv4	554	Fragmented IP protocol (proto=ICMP 1, off=2960, ID=3aa2)

18. What fields change in the IP header among the fragments? Provide screenshot(s) to illustrate and support your answer.

The fields that change in the IP header are the total length, fragment offset, and flags.


```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 1500
Identification: 0x3aa2 (15010)
▼ Flags: 0x20, More fragments
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12
```

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 1500
Identification: 0x3aa2 (15010)
▼ Flags: 0x20, More fragments
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
...0 0101 1100 1000 = Fragment Offset: 1480
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12
```

```
Internet Protocol Version 4, Src: 192.168.50.31, 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: 540
Identification: 0x3aa2 (15010)
▼ Flags: 0x01
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
...0 1011 1001 0000 = Fragment Offset: 2960
Time to Live: 255
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.50.31
Destination Address: 128.119.245.12
```