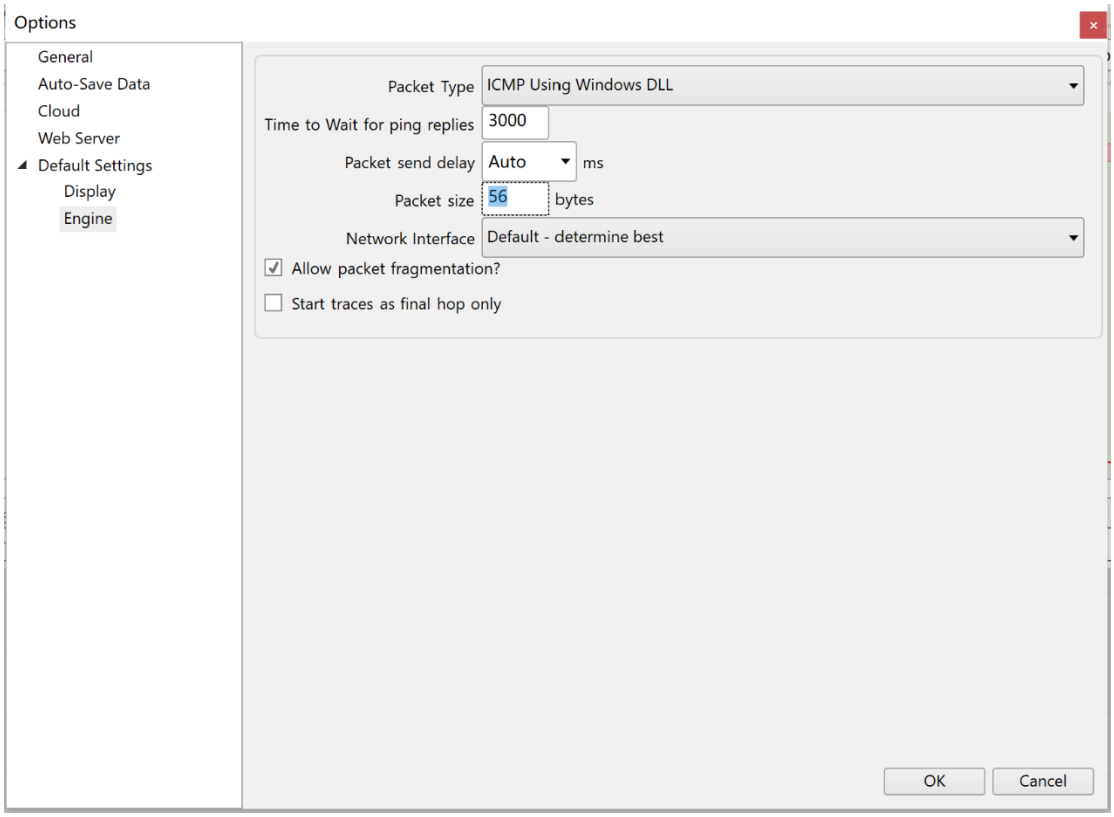
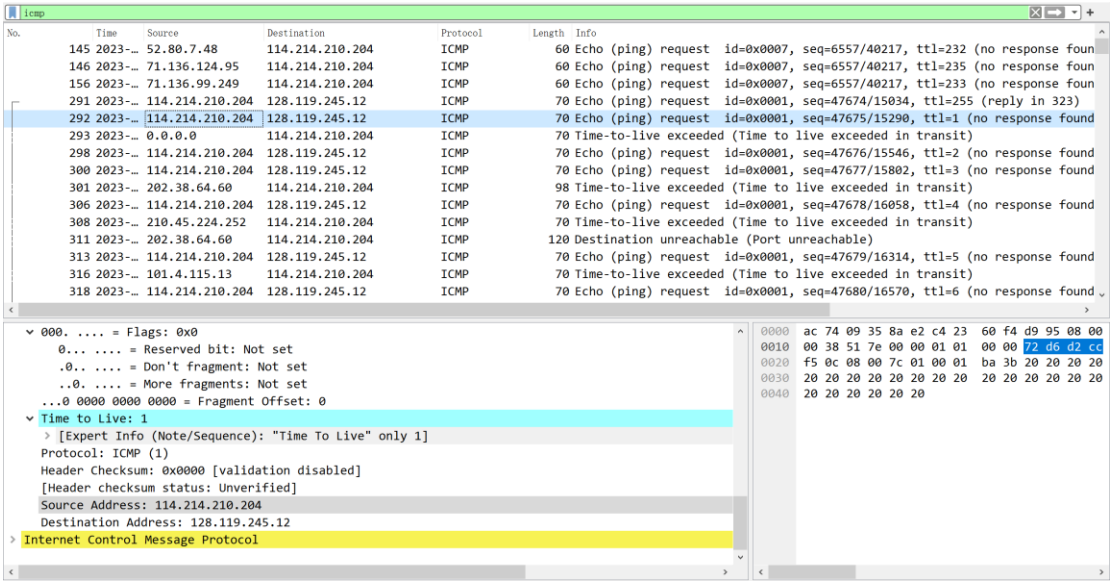
IP 实验

姓名：陈鸿绪　　学号：PB21000224　　日期：11.24.2023

修改发送数据包大小：



1. 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?



IP：114.214.210.204

2. Within the IP packet header, what is the value in the upper layer protocol field?

```
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 114.214.210.204
```

ICMP 为上层协议

3. 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.

```
.... 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: 56
```

Header：20　总长度：56 有效负载：36

4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented

292	2023-…	114.214.210.204	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=47675/15290, ttl=1 (no response
293	2023-…	0.0.0.0	114.214.210.204	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
298	2023-…	114.214.210.204	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=47676/15546, ttl=2 (no response
300	2023-…	114.214.210.204	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=47677/15802, ttl=3 (no response
301	2023-…	202.38.64.60	114.214.210.204	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
306	2023-…	114.214.210.204	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=47678/16058, ttl=4 (no response
308	2023-…	210.45.224.252	114.214.210.204	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
311	2023-…	202.38.64.60	114.214.210.204	ICMP	120	Destination unreachable (Port unreachable)
313	2023-…	114.214.210.204	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=47679/16314, ttl=5 (no response

没有发现多个相同的 TTL，所以并没有分割

5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?

```
Total Length: 56
Identification: 0x517e (20862)
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 1]
      ["Time To Live" only 1]
      [Severity level: Note]
      [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
```

```
Identification: 0x517f (20863)
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: 2
  [Expert Info (Note/Sequence): "Time To Live" only 2]
      ["Time To Live" only 2]
      [Severity level: Note]
      [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
```

可以发现 Time to live、Identification 是不一样的（理论上 Header Checksum 也是会变，不知道为什么这里直接取 0）

6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?

   保持不变：显式拥塞通告(ECN)、全长、标志、分片偏移(fragment offset)、源地址(Source)、目的地址、选项。以上下次可能会改变。

   必须保持不变：版本、首部长度(Internet Header Length)、区分服务(Differentiated Services)、协议。

   必须更改：标识符、存活时间、首部检验和、负载数据

7. Describe the pattern you see in the values in the Identification field of the IP datagram

   Next(with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.

   根据观察不同报文 Identification 不一样。标识符主要用来标识一个报文的所有分片，因此对于不同报文就需要改变该值。

101.4.112.61	114.214.210.204	ICMP	70 Time-to-live exceeded (Time to live exceeded in
101.4.112.61	114.214.210.204	ICMP	70 Time-to-live exceeded (Time to live exceeded in
101.4.112.61	114.214.210.204	ICMP	70 Time-to-live exceeded (Time to live exceeded in
101.4.112.61	114.214.210.204	ICMP	70 Time-to-live exceeded (Time to live exceeded in

8. What is the value in the Identification field and the TTL field?

   如下图所示：

```
Identification: 0x0375 (885)
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: 248
```

9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?

```
Identification: 0x0375 (885)
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: 248
```

```
Identification: 0x0108 (264)
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: 248
```

Identification 有改变，TTL 不变。因为一个路由中的数据包具有相同的寿命，而除分段的数据其他数据包都会有唯一的标识，标识相同表示他们来自同一个数据包的分片。

10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?

本人的实验过程中并没有分片。从第十题开始，所以采用实验提供的数据。

```
192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
192.168.1.102   128.59.23.100   ICMP    562 Echo (ping) request  id=0x0300, seq=30467/887, ttl=1 (no response found!)
```

可以发现第一个 ICMP Echo 请求确实分片了。分成了以上两片。

11. Print out 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

```
192.168.1.102   128.59.23.100   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=32f9) [Reassembled in #93]
001. .... = Flags: 0x1, 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: 1
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: 1500
Identification: 0x32f9 (13049)
```

More fragments 指示有分割，fragment offset 为 0 表示偏移量为 0，即为第一个数据

报片段，总长度为 1500。

12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?

```
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0000 1011 1001 = Fragment Offset: 1480
```

More fragment:Not set 表示数据报不再被分段，*Fragment Offset:1480* 表示其偏移 1480，为第二个分段。

13. What fields change in the IP header between the first and second fragment

total Length、Flags、Header Checksum 均发生了改变

```
Total Length: 1500
Identification: 0x32f9 (13049)
001. .... = Flags: 0x1, 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: 1
    [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x077b [validation disabled]
```

```
Total Length: 548
Identification: 0x32f9 (13049)
000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 1
    [Expert Info (Note/Sequence): "Time To Live" only 1]
        ["Time To Live" only 1]
        [Severity level: Note]
        [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x2a7a [validation disabled]
```

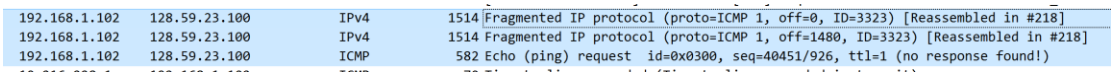
total Length：1500 和 548

Flags：0x0 和 0x1

Header Checksum：0x077b 和 0x2a7a

14. How many fragments were created from the original datagram?

3 个 fragments




```
[3 IPv4 Fragments (3508 bytes): #216(1480), #217(1480), #218(548)]
  [Frame: 216, payload: 0-1479 (1480 bytes)]
  [Frame: 217, payload: 1480-2959 (1480 bytes)]
  [Frame: 218, payload: 2960-3507 (548 bytes)]
  [Fragment count: 3]
  [Reassembled IPv4 length: 3508]
  [Reassembled IPv4 data: 0800a9c303009e03373920aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

15. What fields change in the IP header among the fragments?

分片 1

```
Total Length: 1500
Identification: 0x3323 (13091)
001. .... = Flags: 0x1, 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: 1
  [Expert Info (Note/Sequence): "Time To Live" only 1]
    ["Time To Live" only 1]
    [Severity level: Note]
    [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0751 [validation disabled]
```

分片 2

```
Total Length: 1500
Identification: 0x3323 (13091)
001. .... = Flags: 0x1, More fragments
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
...0 0000 1011 1001 = Fragment Offset: 1480
Time to Live: 1
  [Expert Info (Note/Sequence): "Time To Live" only 1]
    ["Time To Live" only 1]
    [Severity level: Note]
    [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x0698 [validation disabled]
[Header checksum status: Unverified]
```

分片 3

```
Total Length: 568
Identification: 0x3323 (13091)
000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
...0 0001 0111 0010 = Fragment Offset: 2960
Time to Live: 1
  [Expert Info (Note/Sequence): "Time To Live" only 1]
    ["Time To Live" only 1]
    [Severity level: Note]
    [Group: Sequence]
Protocol: ICMP (1)
Header Checksum: 0x2983 [validation disabled]
```

有图可以发现 total length、Identification、flags、header checksum 均有改变