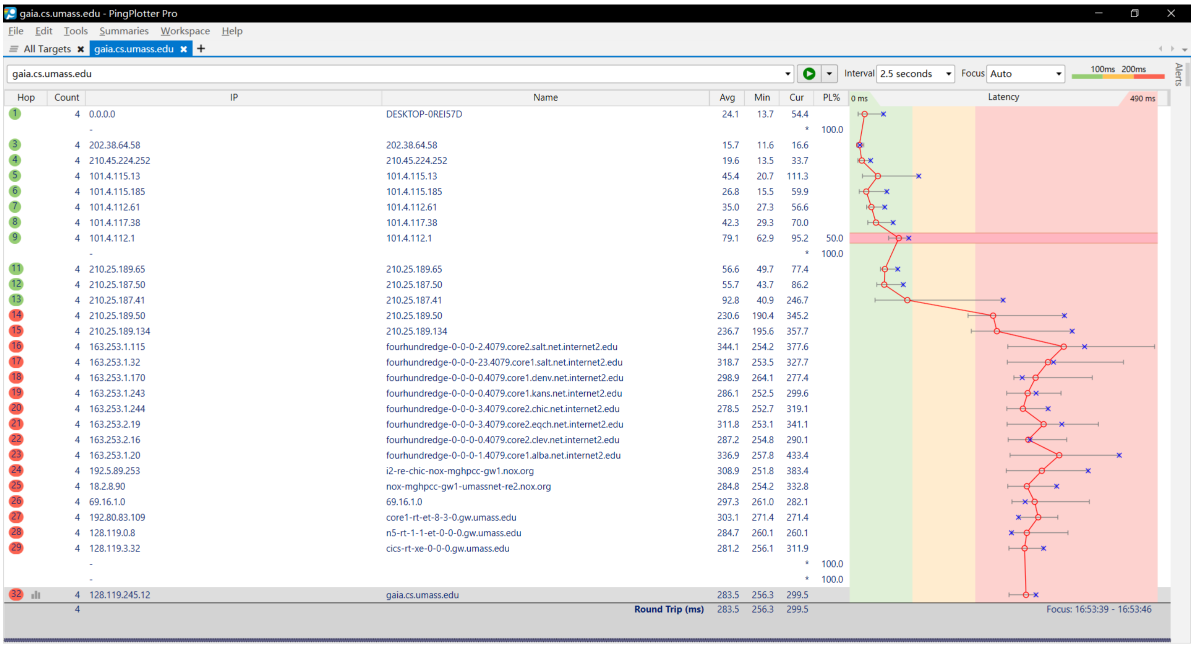
traceroute实验

实验要求

Submit to bb.ustc.edu.cn

- A pdf file named “id + name + traceroute.pdf”
- The packet trace you have captured.
- Your answers to the questions
- For Q1, you need to give the screenshot of the result after performing filter rules and packet with the application-layer protocol.
- For Q2- Q6, you need to give the corresponding screenshot and explanation.
- deadline: 2021/11/30

The packet trace you have captured:



gaia.cs.umass.edu - PingPlotter Pro

gaia.cs.umass.edu

Interval 2.5 seconds

Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	4	0.0.0.0	DESKTOP-0REI57D	24.1	13.7	54.4	
		-				*	100.0
3	4	202.38.64.58	202.38.64.58	15.7	11.6	16.6	
4	4	210.45.224.252	210.45.224.252	19.6	13.5	33.7	
5	4	101.4.115.13	101.4.115.13	45.4	20.7	111.3	
6	4	101.4.115.185	101.4.115.185	26.8	15.5	59.9	
7	4	101.4.112.61	101.4.112.61	35.0	27.3	56.6	
8	4	101.4.117.38	101.4.117.38	42.3	29.3	70.0	
9	4	101.4.112.1	101.4.112.1	79.1	62.9	95.2	50.0
		-				*	100.0
11	4	210.25.189.65	210.25.189.65	56.6	49.7	77.4	
12	4	210.25.187.50	210.25.187.50	55.7	43.7	86.2	
13	4	210.25.187.41	210.25.187.41	92.8	40.9	246.7	
14	4	210.25.189.50	210.25.189.50	230.6	190.4	345.2	
15	4	210.25.189.134	210.25.189.134	236.7	195.6	357.7	
16	4	163.253.1.115	fourhundredge-0-0-0-2.4079.core2.salt.net.internet2.edu	344.1	254.2	377.6	
17	4	163.253.1.32	fourhundredge-0-0-0-23.4079.core1.salt.net.internet2.edu	318.7	253.5	327.7	
18	4	163.253.1.170	fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu	298.9	264.1	277.4	
19	4	163.253.1.243	fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu	286.1	252.5	299.6	
20	4	163.253.1.244	fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu	278.5	252.7	319.1	
21	4	163.253.2.19	fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu	311.8	253.1	341.1	
22	4	163.253.2.16	fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu	287.2	254.8	290.1	
23	4	163.253.1.20	fourhundredge-0-0-0-1.4079.core1.alba.net.internet2.edu	336.9	257.8	433.4	
24	4	192.5.89.253	i2-re-chic-nox-mghpcc-gw1.nox.org	308.9	251.8	383.4	
25	4	18.2.8.90	nox-mghpcc-gw1-umassnet-re2.nox.org	284.8	254.2	332.8	
26	4	69.16.1.0	69.16.1.0	297.3	261.0	282.1	
27	4	192.80.83.109	core1-rt-et-8-3-0.gw.umass.edu	303.1	271.4	271.4	
28	4	128.119.0.8	n5-rt-1-1-et-0-0-0.gw.umass.edu	284.7	260.1	260.1	
29	4	128.119.3.32	cics-rt-xe-0-0-0.gw.umass.edu	281.2	256.1	311.9	
		-				*	100.0
		-				*	100.0
32	4	128.119.245.12	gaia.cs.umass.edu	283.5	256.3	299.5	
	4		Round Trip (ms)	283.5	256.3	299.5	

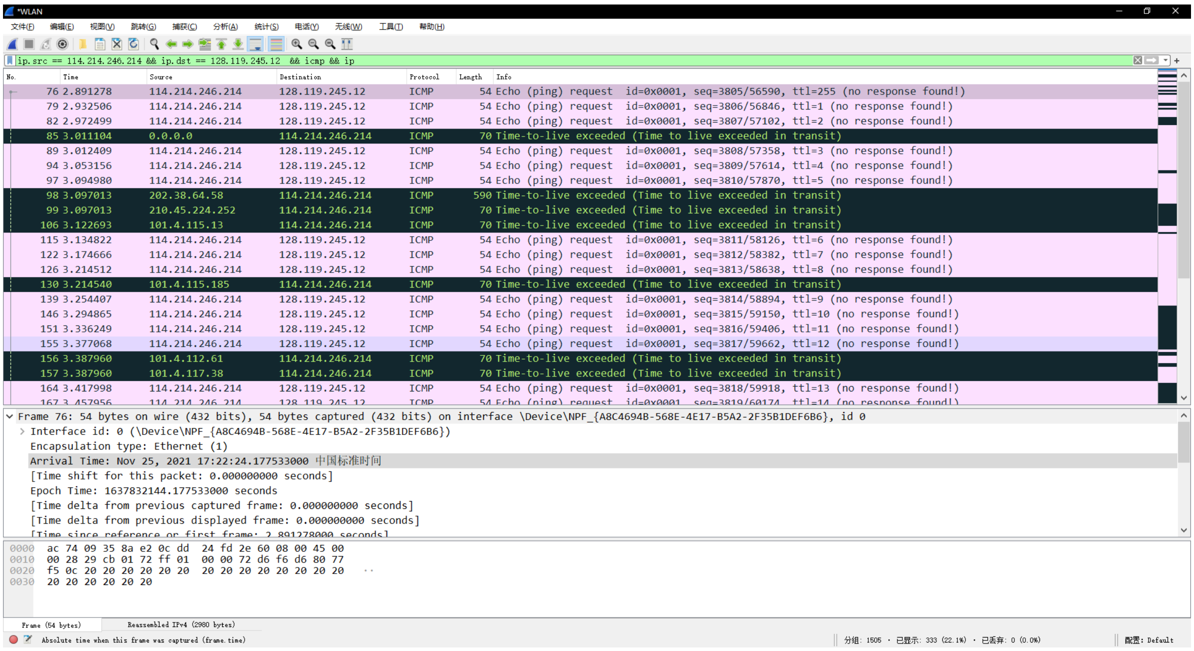
Q&A:

1. Display the rules to filter the IP and ICMP packets between source host and destination host. Are there any other Application-layer protocols when you traceroute gaia.cs.umass.edu?

rules:

ip.src == 114.214.246.214 && ip.dst == 128.119.245.12 && icmp && ip

screenshot:

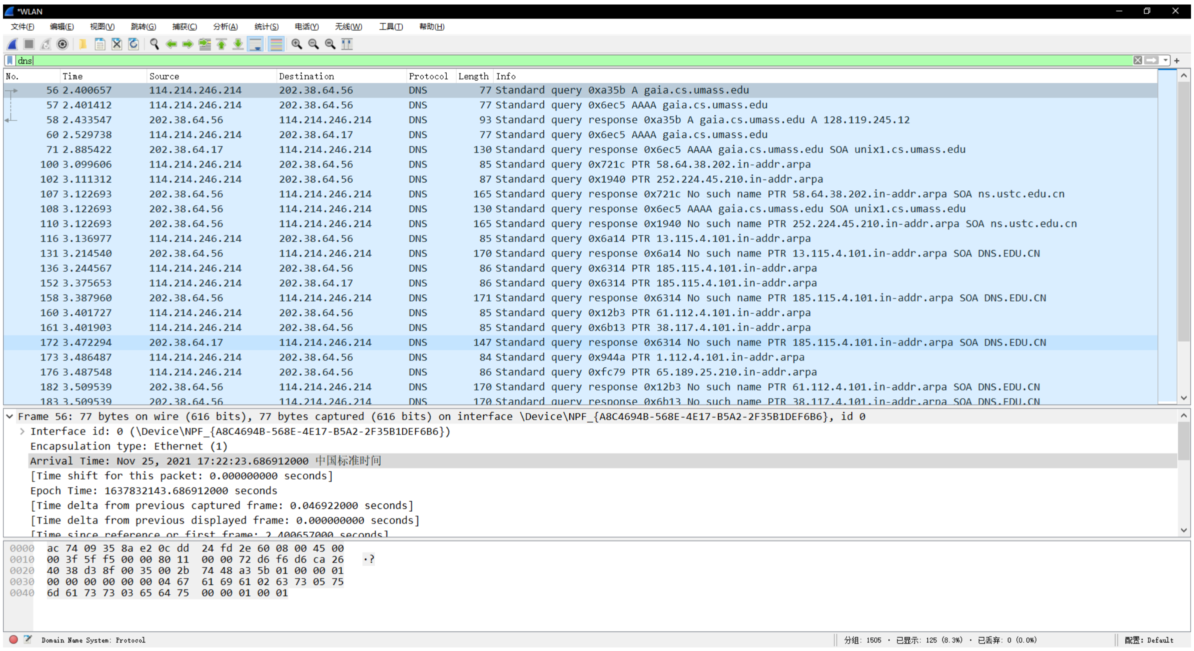

*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

```
ip.src == 114.214.246.214 && ip.dst == 128.119.245.12  && icmp && ip

No.   Time       Source           Destination       Protocol  Length Info
   76 2.891278   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3805/56590, ttl=255 (no response found!)
   79 2.932506   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3806/56846, ttl=1 (no response found!)
   82 2.972499   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3807/57102, ttl=2 (no response found!)
   85 3.011104   0.0.0.0          114.214.246.214   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
   89 3.012409   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3808/57358, ttl=3 (no response found!)
   94 3.053156   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3809/57614, ttl=4 (no response found!)
   97 3.094980   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3810/57870, ttl=5 (no response found!)
   98 3.097013   202.38.64.58     114.214.246.214   ICMP     590 Time-to-live exceeded (Time to live exceeded in transit)
   99 3.097013   210.45.224.252   114.214.246.214   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  106 3.122693   101.4.115.13     114.214.246.214   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  115 3.134822   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3811/58126, ttl=6 (no response found!)
  122 3.174666   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3812/58382, ttl=7 (no response found!)
  126 3.214512   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3813/58638, ttl=8 (no response found!)
  130 3.214540   101.4.115.185    114.214.246.214   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  139 3.254407   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3814/58894, ttl=9 (no response found!)
  146 3.294865   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3815/59150, ttl=10 (no response found!)
  151 3.336249   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3816/59406, ttl=11 (no response found!)
  155 3.377068   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3817/59662, ttl=12 (no response found!)
  156 3.387960   101.4.112.61     114.214.246.214   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  157 3.387960   101.4.117.38     114.214.246.214   ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
  164 3.417998   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3818/59918, ttl=13 (no response found!)
  167 3.457956   114.214.246.214  128.119.245.12    ICMP      54 Echo (ping) request  id=0x0001, seq=3819/60174, ttl=14 (no response found!)

v Frame 76: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{A8C4694B-568E-4E17-B5A2-2F35B1DEF6B6}, id 0
  > Interface id: 0 (\Device\NPF_{A8C4694B-568E-4E17-B5A2-2F35B1DEF6B6})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 25, 2021 17:22:24.177533000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1637832144.177533000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.891278000 seconds]

0000  ac 74 09 35 8a e2 0c dd  24 fd 2e 60 08 00 45 00
0010  00 28 29 cb 01 72 ff 01  00 00 72 d6 f6 d6 80 77
0020  f5 0c 20 20 20 20 20 20  20 20 20 20 20 20 20 20     ··
0030  20 20 20 20 20 20

Frame (54 bytes)    Reassembled IPv4 (2980 bytes)
Absolute time when this frame was captured (frame.time)        分组: 1505 · 已显示: 333 (22.1%) · 已丢弃: 0 (0.0%)        配置: Default
```

other application layer protocols:

DNS protocol.

screenshot:


*WLAN
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

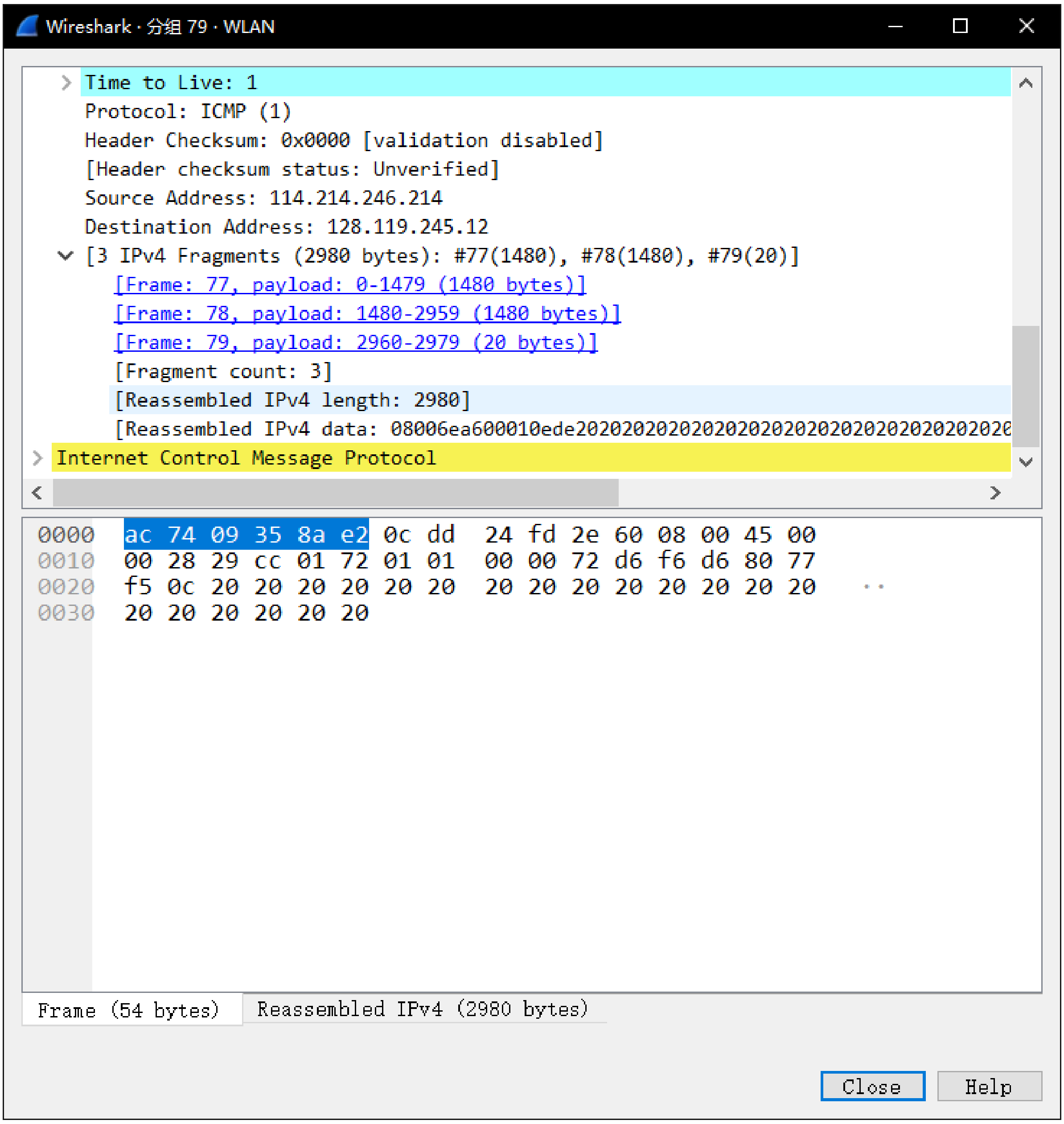
```
dns

No.   Time       Source           Destination       Protocol  Length Info
   56 2.400657   114.214.246.214  202.38.64.56      DNS       77 Standard query 0xa35b A gaia.cs.umass.edu
   57 2.401412   114.214.246.214  202.38.64.56      DNS       77 Standard query 0x6ec5 AAAA gaia.cs.umass.edu
   58 2.433547   202.38.64.56     114.214.246.214   DNS       93 Standard query response 0xa35b A gaia.cs.umass.edu A 128.119.245.12
   60 2.529738   114.214.246.214  202.38.64.17      DNS       77 Standard query 0x6ec5 AAAA gaia.cs.umass.edu
   71 2.885422   202.38.64.17     114.214.246.214   DNS      130 Standard query response 0x6ec5 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
  100 3.099606   114.214.246.214  202.38.64.56      DNS       85 Standard query 0x721c PTR 58.64.38.202.in-addr.arpa
  102 3.111312   114.214.246.214  202.38.64.56      DNS       87 Standard query 0x1940 PTR 252.224.45.210.in-addr.arpa
  107 3.122693   202.38.64.56     114.214.246.214   DNS      165 Standard query response 0x721c No such name PTR 58.64.38.202.in-addr.arpa SOA ns.ustc.edu.cn
  108 3.122693   202.38.64.56     114.214.246.214   DNS      130 Standard query response 0x6ec5 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
  110 3.122693   202.38.64.56     114.214.246.214   DNS      165 Standard query response 0x1940 No such name PTR 252.224.45.210.in-addr.arpa SOA ns.ustc.edu.cn
  116 3.136977   114.214.246.214  202.38.64.56      DNS       85 Standard query 0x6a14 PTR 13.115.4.101.in-addr.arpa
  131 3.214540   202.38.64.56     114.214.246.214   DNS      170 Standard query response 0x6a14 No such name PTR 13.115.4.101.in-addr.arpa SOA DNS.EDU.CN
  136 3.244567   114.214.246.214  202.38.64.56      DNS       86 Standard query 0x6314 PTR 185.115.4.101.in-addr.arpa
  152 3.375653   114.214.246.214  202.38.64.17      DNS       86 Standard query 0x6314 PTR 185.115.4.101.in-addr.arpa
  158 3.387960   202.38.64.56     114.214.246.214   DNS      171 Standard query response 0x6314 No such name PTR 185.115.4.101.in-addr.arpa SOA DNS.EDU.CN
  160 3.401727   114.214.246.214  202.38.64.56      DNS       85 Standard query 0x12b3 PTR 61.112.4.101.in-addr.arpa
  161 3.401903   114.214.246.214  202.38.64.56      DNS       85 Standard query 0x6b13 PTR 38.117.4.101.in-addr.arpa
  172 3.472294   202.38.64.17     114.214.246.214   DNS      147 Standard query response 0x6314 No such name PTR 185.115.4.101.in-addr.arpa SOA DNS.EDU.CN
  173 3.486487   114.214.246.214  202.38.64.56      DNS       84 Standard query 0x944a PTR 1.112.4.101.in-addr.arpa
  176 3.487548   114.214.246.214  202.38.64.56      DNS       86 Standard query 0xfc79 PTR 65.189.25.210.in-addr.arpa
  182 3.509539   202.38.64.56     114.214.246.214   DNS      170 Standard query response 0x12b3 No such name PTR 61.112.4.101.in-addr.arpa SOA DNS.EDU.CN
  183 3.509539   202.38.64.56     114.214.246.214   DNS      170 Standard query response 0x6b13 No such name PTR 38.117.4.101.in-addr.arpa SOA DNS.EDU.CN

v Frame 56: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF_{A8C4694B-568E-4E17-B5A2-2F35B1DEF6B6}, id 0
  > Interface id: 0 (\Device\NPF_{A8C4694B-568E-4E17-B5A2-2F35B1DEF6B6})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 25, 2021 17:22:23.686912000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1637832143.686912000 seconds
    [Time delta from previous captured frame: 0.046922000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 2.400657000 seconds]

0000  ac 74 09 35 8a e2 0c dd  24 fd 2e 60 08 00 45 00
0010  00 3f 5f f5 00 00 80 11  00 00 72 d6 f6 d6 ca 26     ·?
0020  40 38 d3 8f 00 35 00 2b  74 48 a3 5b 01 00 00 01
0030  00 00 00 00 00 00 04 67  61 69 61 02 63 73 05 75
0040  6d 61 73 73 03 65 64 75  00 00 01 00 01

Domain Name System: Protocol        分组: 1505 · 已显示: 125 (8.3%) · 已丢弃: 0 (0.0%)        配置: Default
```

2. How many hops between source and destination? Find the first ICMP Echo Request packet that has TTL=1, is this packet fragmented? If yes, how many fragments, and why is the packet fragmented?

hops: 30

is this packet fragmented? yes

fragment count: 3（见下图）



```
  > Time to Live: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.246.214
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (2980 bytes): #77(1480), #78(1480), #79(20)]
      [Frame: 77, payload: 0-1479 (1480 bytes)]
      [Frame: 78, payload: 1480-2959 (1480 bytes)]
      [Frame: 79, payload: 2960-2979 (20 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2980]
      [Reassembled IPv4 data: 08006ea600010ede202020202020202020202020202020202020202
> Internet Control Message Protocol
```

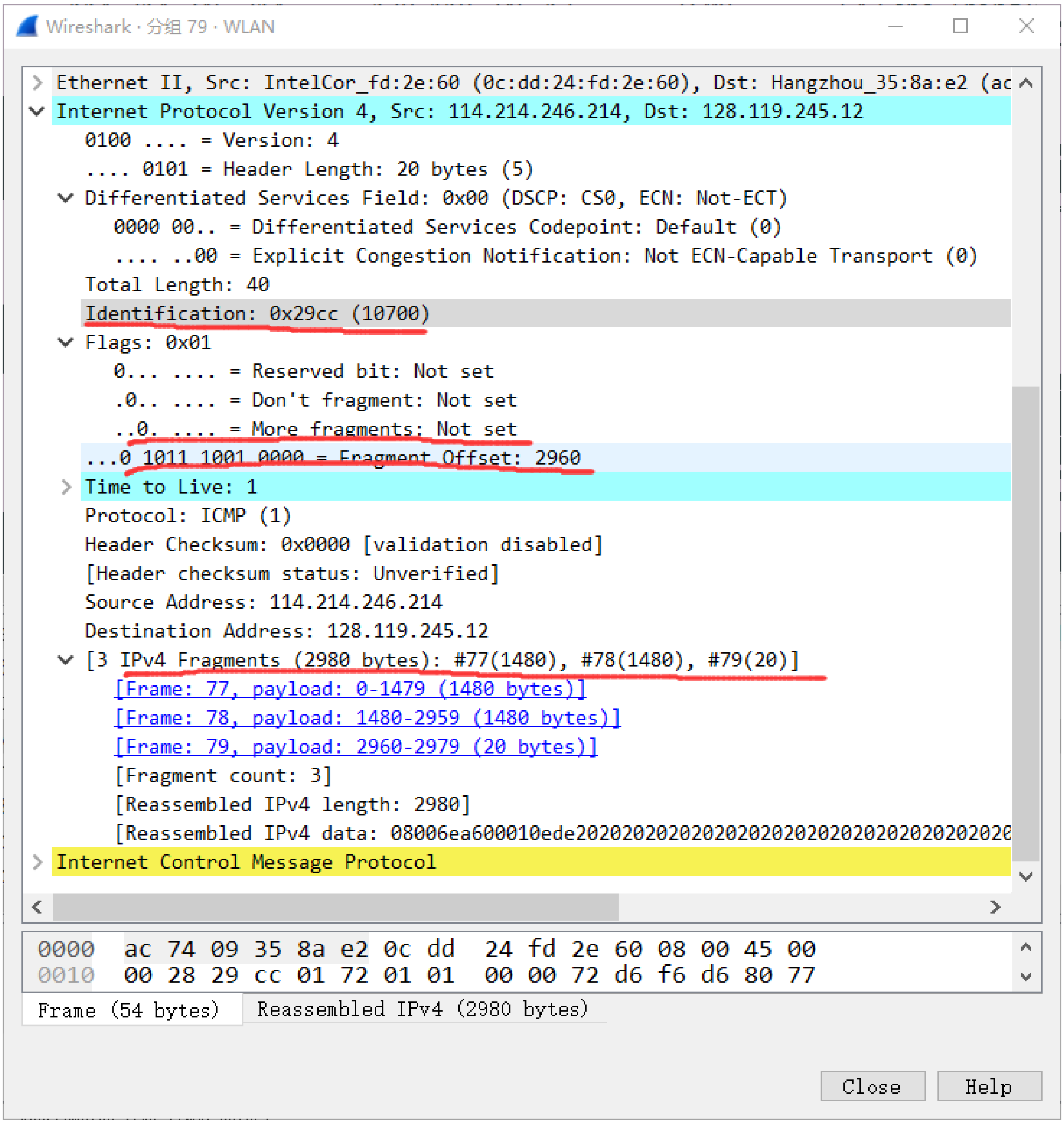
```
0000  ac 74 09 35 8a e2 0c dd  24 fd 2e 60 08 00 45 00
0010  00 28 29 cc 01 72 01 01  00 00 72 d6 f6 d6 80 77
0020  f5 0c 20 20 20 20 20 20  20 20 20 20 20 20 20 20    ..
0030  20 20 20 20 20 20
```

why is the packet fragmented?

因为这个IP数据报长度超过了MTU，所以会进行分片。可以看到上图中数据报大小为2980B，被分为3个片，分别为1480B、1480B、20B。

3. How the packets are fragmented and reassembled? For each fragment, how to know if it is the last fragment, and how many bytes are contained in each fragment? Print the packets and answer by highlighting the relevant fields.

当数据报长度大于MTU时，路由器会将数据分为两个或更多个较小的IP数据报，用单独 的链路层帧封装这些较小的IP数据报。重组时在目的主机端系统之中，通过IP数据报的标识、标志、片偏移字段重组。发送主机通常将发送的每个数据报的标识号加1，目的主机就能通过标识号知道它属于哪个大的数据报。最后一片的标志比特设为0其他设为1，用来让目的主机确信已经收到了最后一片。通过片偏移字段指定该片在初始数据报的哪个位置。前两个一个片中有1480bytes，最后一个片有20bytes。如图所示。下图中More fragment（多分片）字段即为标志比特，当路由器对报分进行分片时，除了最后一个分片的MF位设置为0外，其他所有分片的MF位均设置1，以便接收者直到收到MF位为0的分片为止。



```
> Ethernet II, Src: IntelCor_fd:2e:60 (0c:dd:24:fd:2e:60), Dst: Hangzhou_35:8a:e2 (ac
v Internet Protocol Version 4, Src: 114.214.246.214, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v 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: 40
    Identification: 0x29cc (10700)
  v 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: 1
    Protocol: ICMP (1)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 114.214.246.214
    Destination Address: 128.119.245.12
  v [3 IPv4 Fragments (2980 bytes): #77(1480), #78(1480), #79(20)]
      [Frame: 77, payload: 0-1479 (1480 bytes)]
      [Frame: 78, payload: 1480-2959 (1480 bytes)]
      [Frame: 79, payload: 2960-2979 (20 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2980]
      [Reassembled IPv4 data: 08006ea600010ede202020202020202020202020202020202020
> Internet Control Message Protocol

0000  ac 74 09 35 8a e2 0c dd  24 fd 2e 60 08 00 45 00
0010  00 28 29 cc 01 72 01 01  00 00 72 d6 f6 d6 80 77
```

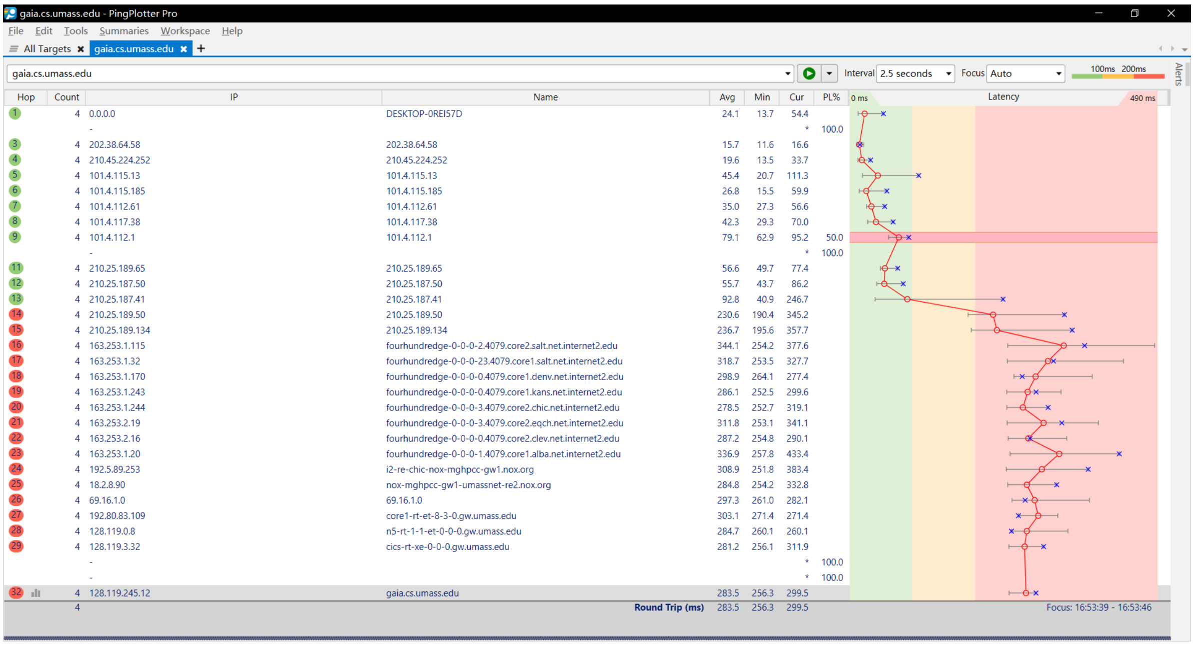
4. What packet is returned from the router when TTL expires? What is contained in the payload of the packet?

当TTL到期时数据报会被丢弃。在有效载荷中包含要交付给目的地的运输层报文段（TCP或UDP），也可能承载其他类型的数据，如ICMP报文。

5. Which link crosses the Pacific, give the router addresses at the two ends of the link. Explained your reason.

two ends: 210.25.187.41 and 210.25.187.50

如图所示：



gaia.cs.umass.edu - PingPlotter Pro
File Edit Tools Summaries Workspace Help
All Targets
gaia.cs.umass.edu
Latency
0 ms
490 ms
100ms 200ms
Alerts

gaia.cs.umass.edu

Interval 2.5 seconds

Focus Auto

Hop	Count	IP	Name	Avg	Min	Cur	PL%
1	4	0.0.0.0	DESKTOP-0REI57D	24.1	13.7	54.4	
		-				*	100.0
3	4	202.38.64.58	202.38.64.58	15.7	11.6	16.6	
4	4	210.45.224.252	210.45.224.252	19.6	13.5	33.7	
5	4	101.4.115.13	101.4.115.13	45.4	20.7	111.3	
6	4	101.4.115.185	101.4.115.185	26.8	15.5	59.9	
7	4	101.4.112.61	101.4.112.61	35.0	27.3	56.6	
8	4	101.4.117.38	101.4.117.38	42.3	29.3	70.0	
9	4	101.4.112.1	101.4.112.1	79.1	62.9	95.2	50.0
		-				*	100.0
11	4	210.25.189.65	210.25.189.65	56.6	49.7	77.4	
12	4	210.25.187.50	210.25.187.50	55.7	43.7	86.2	
13	4	210.25.187.41	210.25.187.41	92.8	40.9	246.7	
14	4	210.25.189.50	210.25.189.50	230.6	190.4	345.2	
15	4	210.25.189.134	210.25.189.134	236.7	195.6	357.7	
16	4	163.253.1.115	fourhundredge-0-0-0-2.4079.core2.salt.net.internet2.edu	344.1	254.2	377.6	
17	4	163.253.1.32	fourhundredge-0-0-0-23.4079.core1.salt.net.internet2.edu	318.7	253.5	327.7	
18	4	163.253.1.170	fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu	298.9	264.1	277.4	
19	4	163.253.1.243	fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu	286.1	252.5	299.6	
20	4	163.253.1.244	fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu	278.5	252.7	319.1	
21	4	163.253.2.19	fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu	311.8	253.1	341.1	
22	4	163.253.2.16	fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu	287.2	254.8	290.1	
23	4	163.253.1.20	fourhundredge-0-0-0-1.4079.core1.alba.net.internet2.edu	336.9	257.8	433.4	
24	4	192.5.89.253	i2-re-chic-nox-mghpcc-gw1.nox.org	308.9	251.8	383.4	
25	4	18.2.8.90	nox-mghpcc-gw1-umassnet-re2.nox.org	284.8	254.2	332.8	
26	4	69.16.1.0	69.16.1.0	297.3	261.0	282.1	
27	4	192.80.83.109	core1-rt-et-8-3-0.gw.umass.edu	303.1	271.4	271.4	
28	4	128.119.0.8	n5-rt-1-1-et-0-0-0.gw.umass.edu	284.7	260.1	260.1	
29	4	128.119.3.32	cics-rt-xe-0-0-0.gw.umass.edu	281.2	256.1	311.9	
		-				*	100.0
		-				*	100.0
32	4	128.119.245.12	gaia.cs.umass.edu	283.5	256.3	299.5	
	4		**Round Trip (ms)**	283.5	256.3	299.5	

Focus: 16:53:39 - 16:53:46

访问210.25.187.41只需92.8ms而到210.25.187.50则需要230.6ms远大于前面的时延，所以肯定是跨海了。

6. How long is the trans-Pacific link? (given that a bit transmits 2*10^8 m/s in fiber).

由5可知，两次的RTT分别为92.8ms与230.6ms：

$$length = \frac{RTT_2 - RTT_1}{2} * v = \frac{230.6ms - 92.8ms}{2} * 2 * 10^8 m/s = 1.378 * 10^7 m$$