# Packet Capture with PingPlotter

吴毅龙 PB19111749

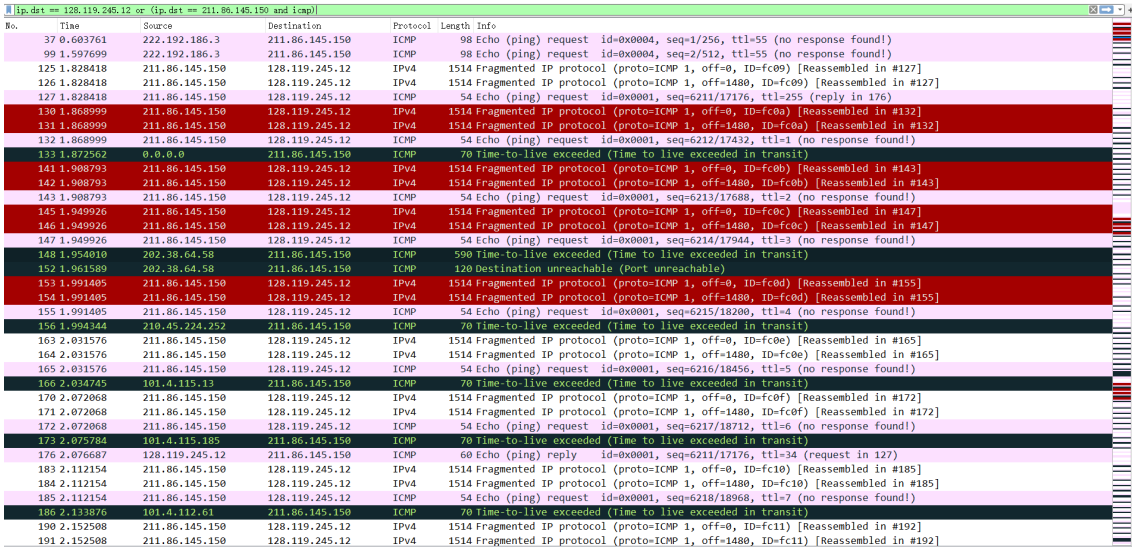
## 1

**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?**

- 过滤源主机和目标主机之间的IP和ICMP数据包的规则为

  `ip.dst == 128.119.245.12 or (ip.dst == 211.86.145.150 and icmp)`

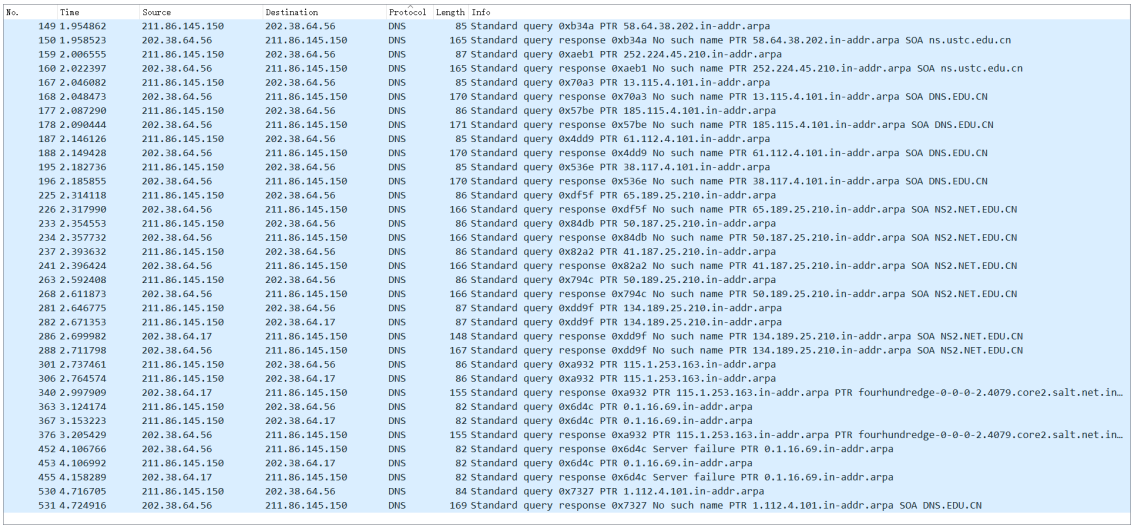
  其中`128.119.245.12`为目的`IP`地址，`211.86.145.150`为源主机`IP`地址



ip.dst == 128.119.245.12 or (ip.dst == 211.86.145.150 and icmp)

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 37 | 0.603761 | 222.192.186.3 | 211.86.145.150 | ICMP | 98 | Echo (ping) request id=0x0004, seq=1/256, ttl=55 (no response found!) |
| 99 | 1.597699 | 222.192.186.3 | 211.86.145.150 | ICMP | 98 | Echo (ping) request id=0x0004, seq=2/512, ttl=55 (no response found!) |
| 125 | 1.828418 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc09) [Reassembled in #127] |
| 126 | 1.828418 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc09) [Reassembled in #127] |
| 127 | 1.828418 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6211/17176, ttl=255 (reply in 176) |
| 130 | 1.868999 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0a) [Reassembled in #132] |
| 131 | 1.868999 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0a) [Reassembled in #132] |
| 132 | 1.868999 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6212/17432, ttl=1 (no response found!) |
| 133 | 1.872562 | 0.0.0.0 | 211.86.145.150 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 141 | 1.908793 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0b) [Reassembled in #143] |
| 142 | 1.908793 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0b) [Reassembled in #143] |
| 143 | 1.908793 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6213/17688, ttl=2 (no response found!) |
| 145 | 1.949926 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0c) [Reassembled in #147] |
| 146 | 1.949926 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0c) [Reassembled in #147] |
| 147 | 1.949926 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6214/17944, ttl=3 (no response found!) |
| 148 | 1.954010 | 202.38.64.58 | 211.86.145.150 | ICMP | 590 | Time-to-live exceeded (Time to live exceeded in transit) |
| 152 | 1.961589 | 202.38.64.58 | 211.86.145.150 | ICMP | 120 | Destination unreachable (Port unreachable) |
| 153 | 1.991405 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0d) [Reassembled in #155] |
| 154 | 1.991405 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0d) [Reassembled in #155] |
| 155 | 1.991405 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6215/18200, ttl=4 (no response found!) |
| 156 | 1.994344 | 210.45.224.252 | 211.86.145.150 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 163 | 2.031576 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0e) [Reassembled in #165] |
| 164 | 2.031576 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0e) [Reassembled in #165] |
| 165 | 2.031576 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6216/18456, ttl=5 (no response found!) |
| 166 | 2.034745 | 101.4.115.13 | 211.86.145.150 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 170 | 2.072068 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0f) [Reassembled in #172] |
| 171 | 2.072068 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0f) [Reassembled in #172] |
| 172 | 2.072068 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6217/18712, ttl=6 (no response found!) |
| 173 | 2.075784 | 101.4.115.185 | 211.86.145.150 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 176 | 2.076687 | 128.119.245.12 | 211.86.145.150 | ICMP | 60 | Echo (ping) reply id=0x0001, seq=6211/17176, ttl=34 (request in 127) |
| 183 | 2.112154 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc10) [Reassembled in #185] |
| 184 | 2.112154 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc10) [Reassembled in #185] |
| 185 | 2.112154 | 211.86.145.150 | 128.119.245.12 | ICMP | 54 | Echo (ping) request id=0x0001, seq=6218/18968, ttl=7 (no response found!) |
| 186 | 2.133876 | 101.4.112.61 | 211.86.145.150 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded in transit) |
| 190 | 2.152508 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc11) [Reassembled in #192] |
| 191 | 2.152508 | 211.86.145.150 | 128.119.245.12 | IPv4 | 1514 | Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc11) [Reassembled in #192] |

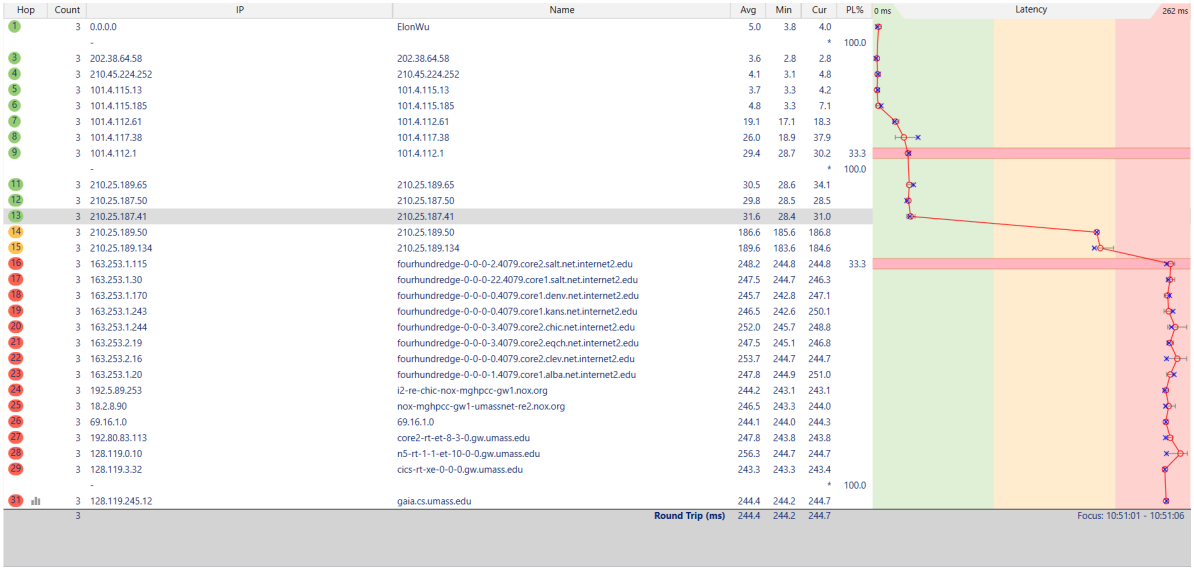
- 跟踪路由`gaia.cs.umass.edu`时还用到的应用层协议有`DNS`



| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 149 | 1.954862 | 211.86.145.150 | 202.38.64.56 | DNS | 85 | Standard query 0xb34a PTR 58.64.38.202.in-addr.arpa |
| 150 | 1.958523 | 202.38.64.56 | 211.86.145.150 | DNS | 165 | Standard query response 0xb34a No such name PTR 58.64.38.202.in-addr.arpa SOA ns.ustc.edu.cn |
| 159 | 2.006555 | 211.86.145.150 | 202.38.64.56 | DNS | 87 | Standard query 0xaeb1 PTR 252.224.45.210.in-addr.arpa |
| 160 | 2.022397 | 202.38.64.56 | 211.86.145.150 | DNS | 165 | Standard query response 0xaeb1 No such name PTR 252.224.45.210.in-addr.arpa SOA ns.ustc.edu.cn |
| 167 | 2.046082 | 211.86.145.150 | 202.38.64.56 | DNS | 85 | Standard query 0x70a3 PTR 13.115.4.101.in-addr.arpa |
| 168 | 2.048473 | 202.38.64.56 | 211.86.145.150 | DNS | 170 | Standard query response 0x70a3 No such name PTR 13.115.4.101.in-addr.arpa SOA DNS.EDU.CN |
| 177 | 2.087290 | 211.86.145.150 | 202.38.64.56 | DNS | 86 | Standard query 0x57be PTR 185.115.4.101.in-addr.arpa |
| 178 | 2.090444 | 202.38.64.56 | 211.86.145.150 | DNS | 171 | Standard query response 0x57be No such name PTR 185.115.4.101.in-addr.arpa SOA DNS.EDU.CN |
| 187 | 2.146126 | 211.86.145.150 | 202.38.64.56 | DNS | 85 | Standard query 0x4dd9 PTR 61.112.4.101.in-addr.arpa |
| 188 | 2.149428 | 202.38.64.56 | 211.86.145.150 | DNS | 170 | Standard query response 0x4dd9 No such name PTR 61.112.4.101.in-addr.arpa SOA DNS.EDU.CN |
| 195 | 2.182736 | 211.86.145.150 | 202.38.64.56 | DNS | 85 | Standard query 0x536e PTR 38.117.4.101.in-addr.arpa |
| 196 | 2.185855 | 202.38.64.56 | 211.86.145.150 | DNS | 170 | Standard query response 0x536e No such name PTR 38.117.4.101.in-addr.arpa SOA DNS.EDU.CN |
| 225 | 2.314118 | 211.86.145.150 | 202.38.64.56 | DNS | 86 | Standard query 0xdf5f PTR 65.189.25.210.in-addr.arpa |
| 226 | 2.317990 | 202.38.64.56 | 211.86.145.150 | DNS | 166 | Standard query response 0xdf5f No such name PTR 65.189.25.210.in-addr.arpa SOA NS2.NET.EDU.CN |
| 233 | 2.354553 | 211.86.145.150 | 202.38.64.56 | DNS | 86 | Standard query 0x84db PTR 50.187.25.210.in-addr.arpa |
| 234 | 2.357732 | 202.38.64.56 | 211.86.145.150 | DNS | 166 | Standard query response 0x84db No such name PTR 50.187.25.210.in-addr.arpa SOA NS2.NET.EDU.CN |
| 237 | 2.393632 | 211.86.145.150 | 202.38.64.56 | DNS | 86 | Standard query 0x82a2 PTR 41.187.25.210.in-addr.arpa |
| 241 | 2.396424 | 202.38.64.56 | 211.86.145.150 | DNS | 166 | Standard query response 0x82a2 No such name PTR 41.187.25.210.in-addr.arpa SOA NS2.NET.EDU.CN |
| 263 | 2.592408 | 211.86.145.150 | 202.38.64.56 | DNS | 86 | Standard query 0x794c PTR 50.189.25.210.in-addr.arpa |
| 268 | 2.611873 | 202.38.64.56 | 211.86.145.150 | DNS | 166 | Standard query response 0x794c No such name PTR 50.189.25.210.in-addr.arpa SOA NS2.NET.EDU.CN |
| 281 | 2.646775 | 211.86.145.150 | 202.38.64.56 | DNS | 87 | Standard query 0xdd9f PTR 134.189.25.210.in-addr.arpa |
| 282 | 2.671353 | 211.86.145.150 | 202.38.64.17 | DNS | 87 | Standard query 0xdd9f PTR 134.189.25.210.in-addr.arpa |
| 286 | 2.699982 | 202.38.64.17 | 211.86.145.150 | DNS | 148 | Standard query response 0xdd9f No such name PTR 134.189.25.210.in-addr.arpa SOA NS2.NET.EDU.CN |
| 288 | 2.711798 | 202.38.64.56 | 211.86.145.150 | DNS | 167 | Standard query response 0xdd9f No such name PTR 134.189.25.210.in-addr.arpa SOA NS2.NET.EDU.CN |
| 301 | 2.737461 | 211.86.145.150 | 202.38.64.56 | DNS | 86 | Standard query 0xa932 PTR 115.1.253.163.in-addr.arpa |
| 306 | 2.764574 | 211.86.145.150 | 202.38.64.17 | DNS | 86 | Standard query 0xa932 PTR 115.1.253.163.in-addr.arpa |
| 340 | 2.997909 | 202.38.64.17 | 211.86.145.150 | DNS | 155 | Standard query response 0xa932 PTR 115.1.253.163.in-addr.arpa PTR fourhundredge-0-0-0-2.4079.core2.salt.net.in… |
| 363 | 3.124174 | 211.86.145.150 | 202.38.64.56 | DNS | 82 | Standard query 0x6d4c PTR 0.1.16.69.in-addr.arpa |
| 367 | 3.153223 | 211.86.145.150 | 202.38.64.17 | DNS | 82 | Standard query 0x6d4c PTR 0.1.16.69.in-addr.arpa |
| 376 | 3.205429 | 202.38.64.56 | 211.86.145.150 | DNS | 155 | Standard query response 0xa932 PTR 115.1.253.163.in-addr.arpa PTR fourhundredge-0-0-0-2.4079.core2.salt.net.in… |
| 452 | 4.106766 | 202.38.64.56 | 211.86.145.150 | DNS | 82 | Standard query response 0x6d4c Server failure PTR 0.1.16.69.in-addr.arpa |
| 453 | 4.106992 | 211.86.145.150 | 202.38.64.17 | DNS | 82 | Standard query 0x6d4c PTR 0.1.16.69.in-addr.arpa |
| 455 | 4.158289 | 202.38.64.17 | 211.86.145.150 | DNS | 82 | Standard query response 0x6d4c Server failure PTR 0.1.16.69.in-addr.arpa |
| 530 | 4.716705 | 211.86.145.150 | 202.38.64.56 | DNS | 84 | Standard query 0x7327 PTR 1.112.4.101.in-addr.arpa |
| 531 | 4.724916 | 202.38.64.56 | 211.86.145.150 | DNS | 169 | Standard query response 0x7327 No such name PTR 1.112.4.101.in-addr.arpa SOA DNS.EDU.CN |

# 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?**



| Hop | Count | IP | Name | Avg | Min | Cur | PL% |
|---|---|---|---|---|---|---|---|
| 1 | 3 | 0.0.0.0 | ElonWu | 5.0 | 3.8 | 4.0 | |
| | | - | | | | * | 100.0 |
| 3 | 3 | 202.38.64.58 | 202.38.64.58 | 3.6 | 2.8 | 2.8 | |
| 4 | 3 | 210.45.224.252 | 210.45.224.252 | 4.1 | 3.1 | 4.8 | |
| 5 | 3 | 101.4.115.13 | 101.4.115.13 | 3.7 | 3.3 | 4.2 | |
| 6 | 3 | 101.4.115.185 | 101.4.115.185 | 4.8 | 3.3 | 7.1 | |
| 7 | 3 | 101.4.112.61 | 101.4.112.61 | 19.1 | 17.1 | 18.3 | |
| 8 | 3 | 101.4.117.38 | 101.4.117.38 | 26.0 | 18.9 | 37.9 | |
| 9 | 3 | 101.4.112.1 | 101.4.112.1 | 29.4 | 28.7 | 30.2 | 33.3 |
| | | - | | | | * | 100.0 |
| 11 | 3 | 210.25.189.65 | 210.25.189.65 | 30.5 | 28.6 | 34.1 | |
| 12 | 3 | 210.25.187.50 | 210.25.187.50 | 29.8 | 28.5 | 28.5 | |
| 13 | 3 | 210.25.187.41 | 210.25.187.41 | 31.6 | 28.4 | 31.0 | |
| 14 | 3 | 210.25.189.50 | 210.25.189.50 | 186.6 | 185.6 | 186.8 | |
| 15 | 3 | 210.25.189.134 | 210.25.189.134 | 189.6 | 183.6 | 184.6 | |
| 16 | 3 | 163.253.1.115 | fourhundredge-0-0-0-2.4079.core2.salt.net.internet2.edu | 248.2 | 244.8 | 244.8 | 33.3 |
| 17 | 3 | 163.253.1.30 | fourhundredge-0-0-0-22.4079.core1.salt.net.internet2.edu | 247.5 | 244.7 | 246.3 | |
| 18 | 3 | 163.253.1.170 | fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu | 245.7 | 242.8 | 247.1 | |
| 19 | 3 | 163.253.1.243 | fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu | 246.5 | 242.6 | 250.1 | |
| 20 | 3 | 163.253.1.244 | fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu | 252.0 | 245.7 | 248.8 | |
| 21 | 3 | 163.253.2.19 | fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu | 247.5 | 245.1 | 246.8 | |
| 22 | 3 | 163.253.2.16 | fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu | 253.7 | 244.7 | 244.7 | |
| 23 | 3 | 163.253.1.20 | fourhundredge-0-0-0-1.4079.core1.alba.net.internet2.edu | 247.8 | 244.9 | 251.0 | |
| 24 | 3 | 192.5.89.253 | i2-re-chic-nox-mghpcc-gw1.nox.org | 244.2 | 243.1 | 243.1 | |
| 25 | 3 | 18.2.8.90 | nox-mghpcc-gw1-umassnet-re2.nox.org | 246.5 | 243.3 | 244.0 | |
| 26 | 3 | 69.16.1.0 | 69.16.1.0 | 244.1 | 244.0 | 244.3 | |
| 27 | 3 | 192.80.83.113 | core2-rt-et-8-3-0.gw.umass.edu | 247.8 | 243.8 | 243.8 | |
| 28 | 3 | 128.119.0.10 | n5-rt-1-1-et-10-0-0.gw.umass.edu | 256.3 | 244.7 | 244.7 | |
| 29 | 3 | 128.119.3.32 | cics-rt-xe-0-0-0.gw.umass.edu | 243.3 | 243.3 | 243.4 | |
| | | - | | | | * | 100.0 |
| 31 | 3 | 128.119.245.12 | gaia.cs.umass.edu | 244.4 | 244.2 | 244.7 | |
| | 3 | | Round Trip (ms) | 244.4 | 244.2 | 244.7 | |

Latency: 0 ms – 262 ms. Focus: 10:51:01 - 10:51:06

- 由上图易知，源主机与目的主机时间有`31`跳
- `TTL=1`的包如下图所示

```
130 1.868999   211.86.145.150   128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=fc0a) [Reassembled in #132]
131 1.868999   211.86.145.150   128.119.245.12   IPv4   1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=fc0a) [Reassembled in #132]
132 1.868999   211.86.145.150   128.119.245.12   ICMP     54 Echo (ping) request  id=0x0001, seq=6212/17432, ttl=1 (no response found!)
```

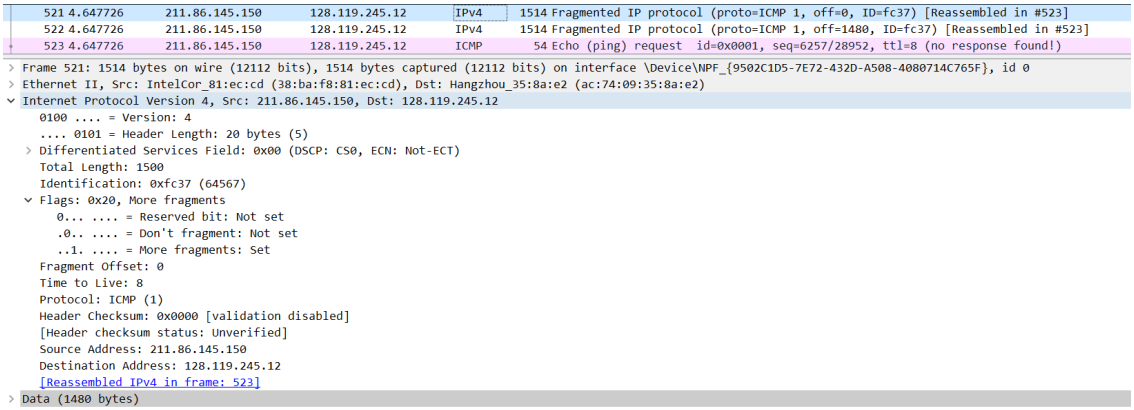
  这个包被分成了3个分片；一个链路层帧能承载的最大数据量叫做**最大传送单元（MTU）**，链路层的MTU限制了IP数据报的长度。所以在源主机上或是路由器上会将IP数据报中的数据分片成两个或更多个较小的IP数据报，用单独的链路层帧封装这些较小的IP数据报，然后向输出链路上发送这些帧。

# 3

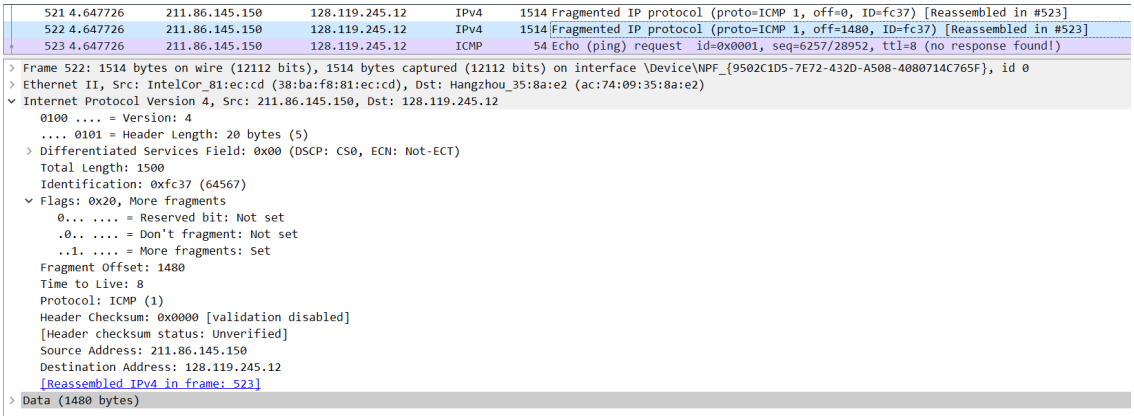
**How the packets are fragmented and reassembled? For each fragment, how to know if it is the last fragment, and how many bytes are contained in each fragment? Print the packets and answer by highlighting the relevant fields.**

- 一个链路层帧能承载的最大数据量叫做**最大传送单元（MTU）**，链路层的MTU限制了IP数据报的长度。所以在源主机上或是路由器上会将IP数据报中的数据分片成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，然后向输出链路上发送这些帧。分片的重新组装工作放到端系统中，而不是在网络路由中。
- 当路由器需要对一个数据报分片时，形成的每个分片具有初始数据报的原地址、目的地址与标识号。**最后一个分片的标志比特被设置为0，其他分片的标志比特为1。**另外使用**偏移字段**可以确定每一个分片在原数据报中的位置。
- 具体到实验结果如下图所示：

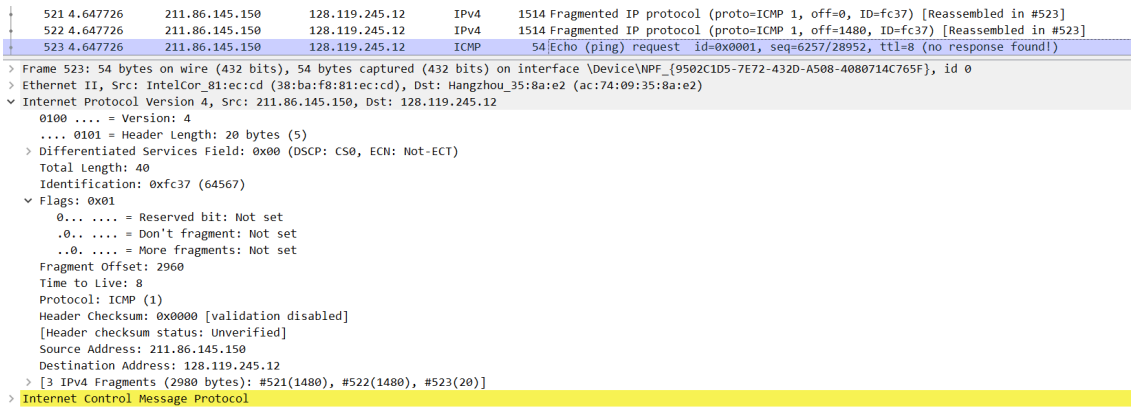
  第一个分片包含`1500byte`，其中`20byte`头部，`1480byte`数据




第二个分片包含`1500byte`，其中`20byte`头部，`1480byte`数据




第三个分片包含`40byte`，其中`20byte`头部，`20byte`数据




从以上三个图中可以很容易看到，三个分片的`Identification: 0xfc37(64567)`，说明三个分片源自同一个包

其中第一个和第二个包的`Flag: 0x20, More fragments`，表示后面还有更多分片；第三个分片的`Flag: 0x01`表示是最后一个分片。

第一个分片`Fragment Offset: 0`，第二个分片`Fragment Offset: 1480`，第三个分片`Fragment Offset: 2960`，是分片在目的主机可以顺利组装

## 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，这一跳路由器会向源主机发送一个`ICMP`包，告知源主机`TTL`已经过期。

```
156 1.994344      210.45.224.252      211.86.145.150      ICMP      70 Time-to-live exceeded (Time to live exceeded in transit)
> Frame 156: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{9502C1D5-7E72-432D-A508-4080714C765F}, id 0
> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_81:ec:cd (38:ba:f8:81:ec:cd)
v Internet Protocol Version 4, Src: 210.45.224.252, Dst: 211.86.145.150
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x01f7 (503)
  > Flags: 0x00
    Fragment Offset: 0
    Time to Live: 252
    Protocol: ICMP (1)
    Header Checksum: 0xa4b6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 210.45.224.252
    Destination Address: 211.86.145.150
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6f7a [correct]
    [Checksum Status: Good]
    Unused: 00000000
  > Internet Protocol Version 4, Src: 211.86.145.150, Dst: 128.119.245.12
  > Internet Control Message Protocol
```

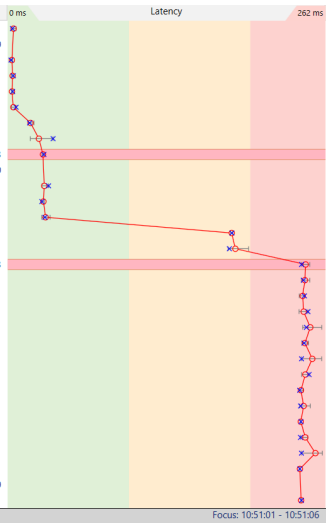
- 包的有效载荷中由`IP`承载`ICMP`报文。如上图所示：`Type: 11(Time-to-live exceeded)`表示接收到的包`TTL`已经过期；`Code: 0(Time-to-live in transit)`表示在`transit`过程中过期；接下来两行表示检验和与检验和无误；后面还包含有过期包的信息（`IP`报文头以及`IP`承载的内容），内容如下图所示。

```
v Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x6f7a [correct]
    [Checksum Status: Good]
    Unused: 00000000
  v Internet Protocol Version 4, Src: 211.86.145.150, 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: 0xfc0d (64525)
    > Flags: 0x20, More fragments
      Fragment Offset: 0
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0xbda2 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 211.86.145.150
      Destination Address: 128.119.245.12
  v Internet Control Message Protocol
      Type: 8 (Echo (ping) request)
      Code: 0
      Checksum: 0x653d [unverified] [in ICMP error packet]
      [Checksum Status: Unverified]
      Identifier (BE): 1 (0x0001)
      Identifier (LE): 256 (0x0100)
      Sequence Number (BE): 6215 (0x1847)
      Sequence Number (LE): 18200 (0x4718)
```

# 5

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

| Hop | Count | IP | Name | Avg | Min | Cur | PL% |
|---|---|---|---|---|---|---|---|
| 1 | 3 | 0.0.0.0 | ElonWu | 5.0 | 3.8 | 4.0 | |
| | | - | | | | * | 100.0 |
| 3 | 3 | 202.38.64.58 | 202.38.64.58 | 3.6 | 2.8 | 2.8 | |
| 4 | 3 | 210.45.224.252 | 210.45.224.252 | 4.1 | 3.1 | 4.8 | |
| 5 | 3 | 101.4.115.13 | 101.4.115.13 | 3.7 | 3.3 | 4.2 | |
| 6 | 3 | 101.4.115.185 | 101.4.115.185 | 4.8 | 3.3 | 7.1 | |
| 7 | 3 | 101.4.112.61 | 101.4.112.61 | 19.1 | 17.1 | 18.3 | |
| 8 | 3 | 101.4.117.38 | 101.4.117.38 | 26.0 | 18.9 | 37.9 | |
| 9 | 3 | 101.4.112.1 | 101.4.112.1 | 29.4 | 28.7 | 30.2 | 33.3 |
| | | - | | | | * | 100.0 |
| 11 | 3 | 210.25.189.65 | 210.25.189.65 | 30.5 | 28.6 | 34.1 | |
| 12 | 3 | 210.25.187.50 | 210.25.187.50 | 29.8 | 28.5 | 28.5 | |
| 13 | 3 | 210.25.187.41 | 210.25.187.41 | 31.6 | 28.4 | 31.0 | |
| 14 | 3 | 210.25.189.50 | 210.25.189.50 | 186.6 | 185.6 | 186.8 | |
| 15 | 3 | 210.25.189.134 | 210.25.189.134 | 189.6 | 183.6 | 184.6 | |
| 16 | 3 | 163.253.1.115 | fourhundredge-0-0-0-2.4079.core2.salt.net.internet2.edu | 248.2 | 244.8 | 244.8 | 33.3 |
| 17 | 3 | 163.253.1.30 | fourhundredge-0-0-0-22.4079.core1.salt.net.internet2.edu | 247.5 | 244.7 | 246.3 | |
| 18 | 3 | 163.253.1.170 | fourhundredge-0-0-0-0.4079.core1.denv.net.internet2.edu | 245.7 | 242.8 | 247.1 | |
| 19 | 3 | 163.253.1.243 | fourhundredge-0-0-0-0.4079.core1.kans.net.internet2.edu | 246.5 | 242.6 | 250.1 | |
| 20 | 3 | 163.253.1.244 | fourhundredge-0-0-0-3.4079.core2.chic.net.internet2.edu | 252.0 | 245.7 | 248.8 | |
| 21 | 3 | 163.253.2.19 | fourhundredge-0-0-0-3.4079.core2.eqch.net.internet2.edu | 247.5 | 245.1 | 246.8 | |
| 22 | 3 | 163.253.2.16 | fourhundredge-0-0-0-0.4079.core2.clev.net.internet2.edu | 253.7 | 244.7 | 244.7 | |
| 23 | 3 | 163.253.1.20 | fourhundredge-0-0-0-1.4079.core1.alba.net.internet2.edu | 247.8 | 244.9 | 251.0 | |
| 24 | 3 | 192.5.89.253 | i2-re-chic-nox-mghpcc-gw1.nox.org | 244.2 | 243.1 | 243.1 | |
| 25 | 3 | 18.2.8.90 | nox-mghpcc-gw1-umassnet-re2.nox.org | 246.5 | 243.3 | 244.0 | |
| 26 | 3 | 69.16.1.0 | 69.16.1.0 | 244.1 | 244.0 | 244.3 | |
| 27 | 3 | 192.80.83.113 | core2-rt-et-8-3-0.gw.umass.edu | 247.8 | 243.8 | 243.8 | |
| 28 | 3 | 128.119.0.10 | n5-rt-1-1-et-10-0-0.gw.umass.edu | 256.3 | 244.7 | 244.7 | |
| 29 | 3 | 128.119.3.32 | cics-rt-xe-0-0-0.gw.umass.edu | 243.3 | 243.3 | 243.4 | |
| | | - | | | | * | 100.0 |
| 31 | 3 | 128.119.245.12 | gaia.cs.umass.edu | 244.4 | 244.2 | 244.7 | |
| | 3 | | **Round Trip (ms)** | 244.4 | 244.2 | 244.7 | |




- `13-14`跳为跨越太平洋的链路，两端路由器的IP分别是`210.25.187.41`和`210.25.189.50`
- 原因：由上图可知，`13`跳以前，包括`14`跳以后的平均时延增幅都比较小，从`13`跳到`14`跳之间平均时延有明显增加。

## 6

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

第`13`跳的平均响应时间为`31.6 ms`，第`14`跳的平均响应时间为`186.6 ms`

则估计太平洋链路的长度为$(186.6-31.6)/1000\times2\times10^8=31000km$