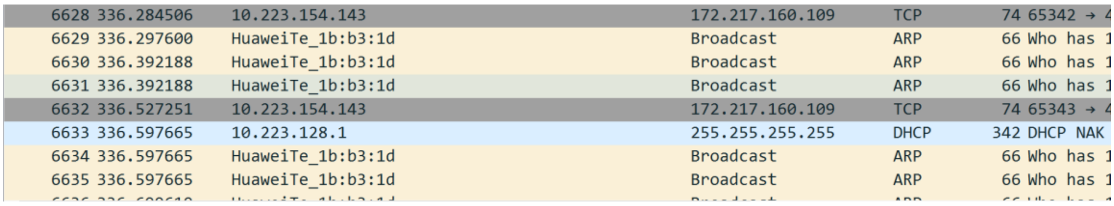
实验一实验报告

20307130112 马成

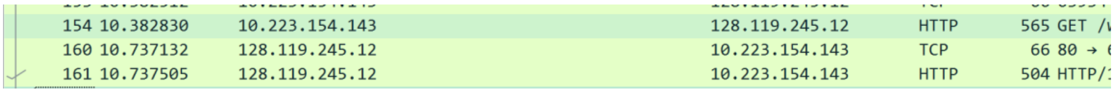
一、 第一问

1. 可以看到下图中有三种 protocols 分别是 ARP、TCP、DHCP



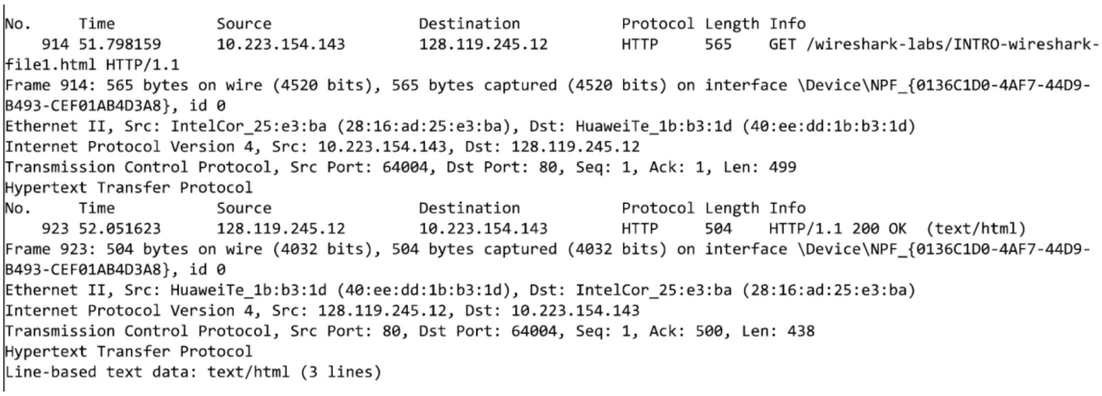
```
6628 336.284506    10.223.154.143        172.217.160.109    TCP     74 65342 → 4
6629 336.297600    HuaweiTe_1b:b3:1d     Broadcast          ARP     66 Who has 1
6630 336.392188    HuaweiTe_1b:b3:1d     Broadcast          ARP     66 Who has 1
6631 336.392188    HuaweiTe_1b:b3:1d     Broadcast          ARP     66 Who has 1
6632 336.527251    10.223.154.143        172.217.160.109    TCP     74 65343 → 4
6633 336.597665    10.223.128.1          255.255.255.255    DHCP   342 DHCP NAK
6634 336.597665    HuaweiTe_1b:b3:1d     Broadcast          ARP     66 Who has 1
6635 336.597665    HuaweiTe_1b:b3:1d     Broadcast          ARP     66 Who has 1
```

2. 两次相差的时间是 10.737505-10.382830=0.354675s



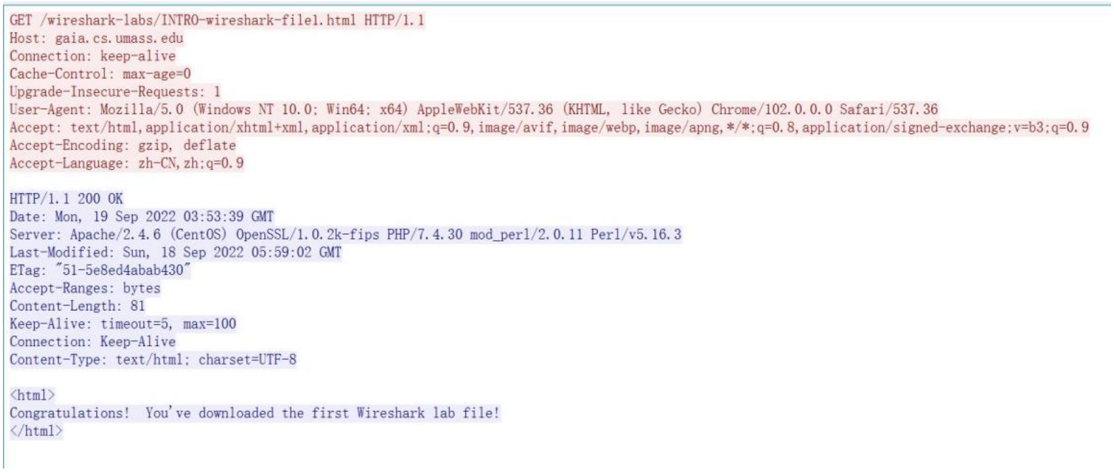
```
154 10.382830    10.223.154.143    128.119.245.12    HTTP    565 GET /w
160 10.737132    128.119.245.12    10.223.154.143    TCP      66 80 → 6
161 10.737505    128.119.245.12    10.223.154.143    HTTP    504 HTTP/1
```

3. 我电脑的 ip 是 10.233.154.143 对方 ip 是 128.119.245.12
4. 打印信息



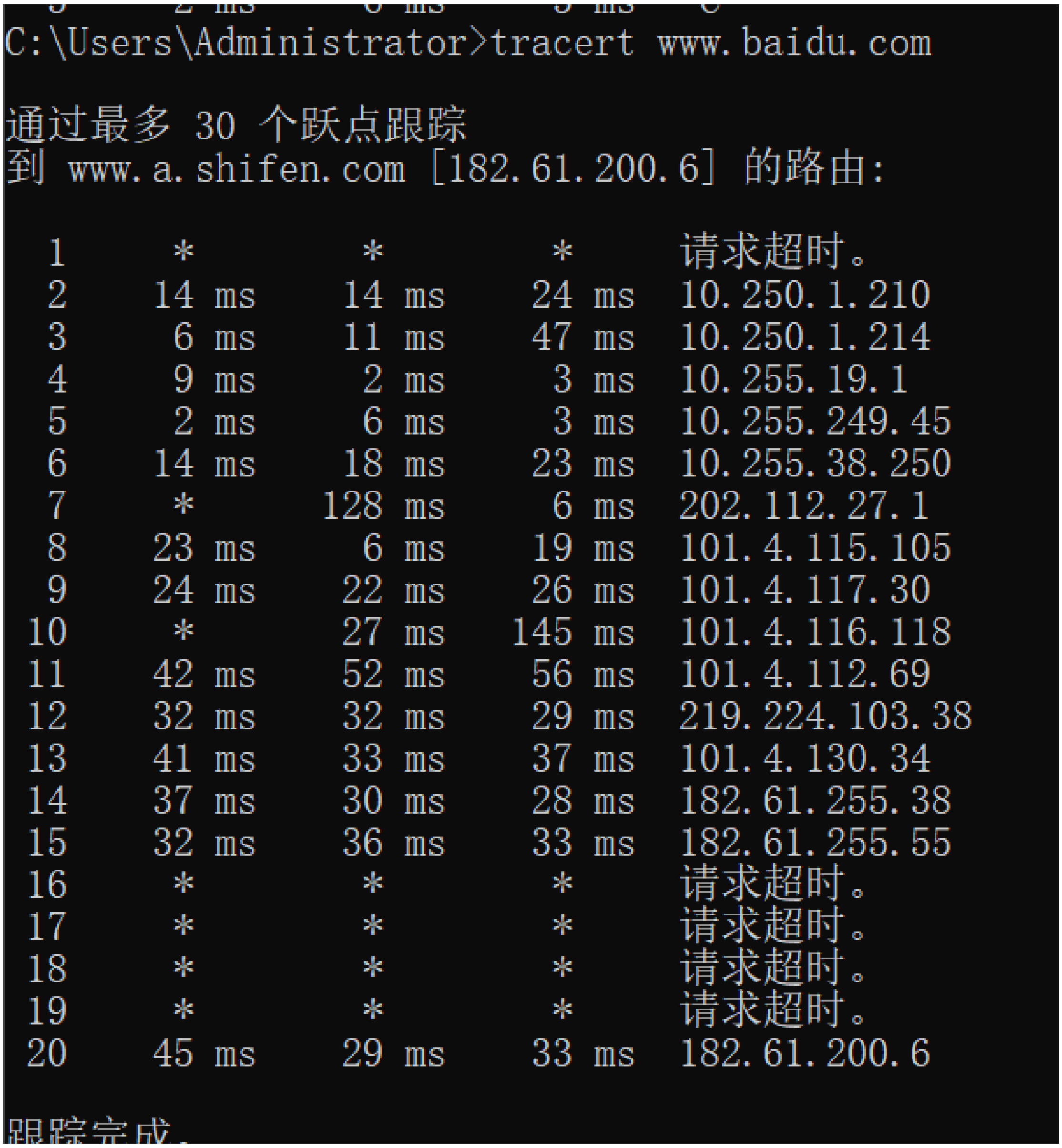
```
No.     Time           Source                Destination           Protocol Length Info
    914 51.798159      10.223.154.143        128.119.245.12        HTTP     565    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 914: 565 bytes on wire (4520 bits), 565 bytes captured (4520 bits) on interface \Device\NPF_{0136C1D0-4AF7-44D9-
B493-CEF01AB4D3A8}, id 0
Ethernet II, Src: IntelCor_25:e3:ba (28:16:ad:25:e3:ba), Dst: HuaweiTe_1b:b3:1d (40:ee:dd:1b:b3:1d)
Internet Protocol Version 4, Src: 10.223.154.143, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64004, Dst Port: 80, Seq: 1, Ack: 1, Len: 499
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    923 52.051623      128.119.245.12        10.223.154.143        HTTP     504    HTTP/1.1 200 OK  (text/html)
Frame 923: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface \Device\NPF_{0136C1D0-4AF7-44D9-
B493-CEF01AB4D3A8}, id 0
Ethernet II, Src: HuaweiTe_1b:b3:1d (40:ee:dd:1b:b3:1d), Dst: IntelCor_25:e3:ba (28:16:ad:25:e3:ba)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.223.154.143
Transmission Control Protocol, Src Port: 80, Dst Port: 64004, Seq: 1, Ack: 500, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
```

二、 第二问

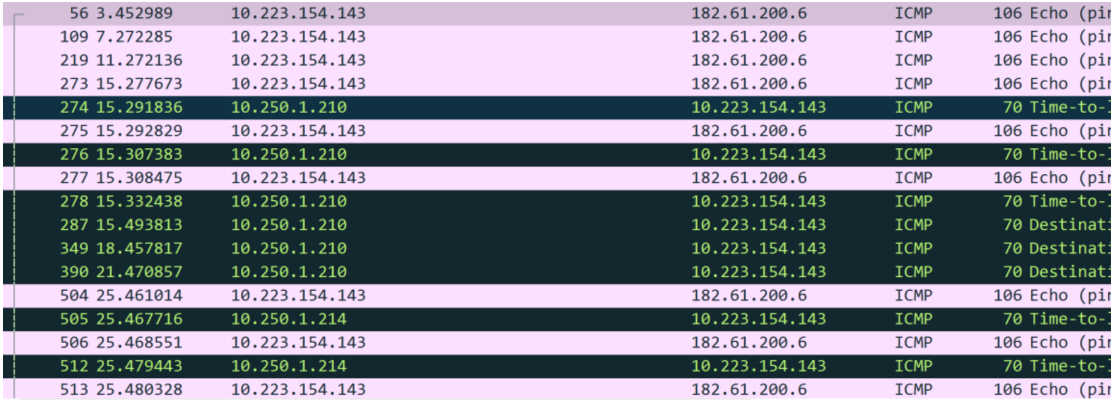


```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

HTTP/1.1 200 OK
Date: Mon, 19 Sep 2022 03:53:39 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sun, 18 Sep 2022 05:59:02 GMT
ETag: "51-5e8ed4abab430"
Accept-Ranges: bytes
Content-Length: 81
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations!  You've downloaded the first Wireshark lab file!
</html>
```

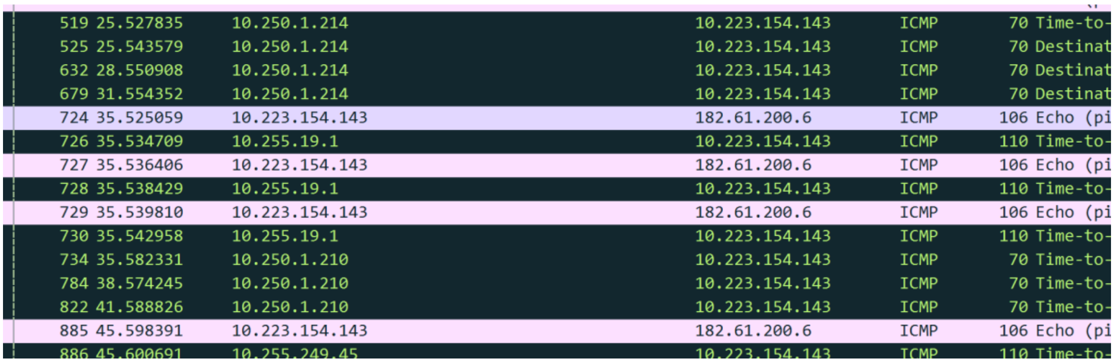
三、 第三问



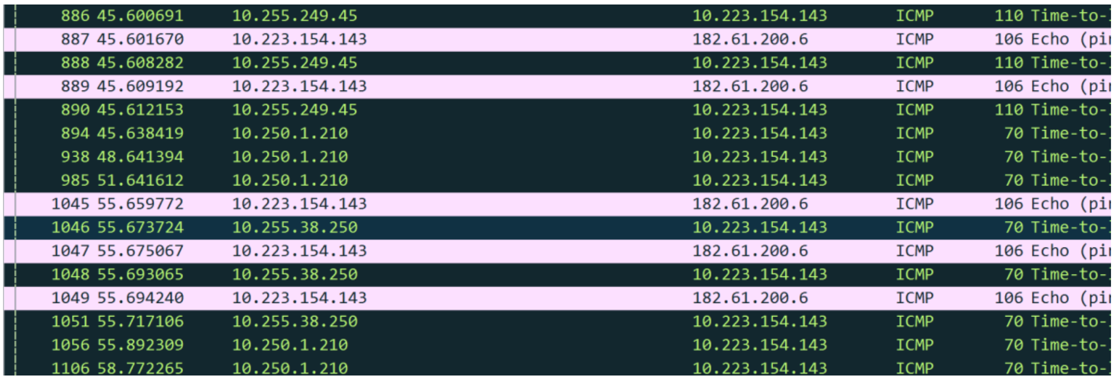
```
C:\Users\Administrator>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.a.shifen.com [182.61.200.6] 的路由:

  1     *        *        *     请求超时。
  2    14 ms    14 ms    24 ms  10.250.1.210
  3     6 ms    11 ms    47 ms  10.250.1.214
  4     9 ms     2 ms     3 ms  10.255.19.1
  5     2 ms     6 ms     3 ms  10.255.249.45
  6    14 ms    18 ms    23 ms  10.255.38.250
  7     *      128 ms     6 ms  202.112.27.1
  8    23 ms     6 ms    19 ms  101.4.115.105
  9    24 ms    22 ms    26 ms  101.4.117.30
 10     *       27 ms   145 ms  101.4.116.118
 11    42 ms    52 ms    56 ms  101.4.112.69
 12    32 ms    32 ms    29 ms  219.224.103.38
 13    41 ms    33 ms    37 ms  101.4.130.34
 14    37 ms    30 ms    28 ms  182.61.255.38
 15    32 ms    36 ms    33 ms  182.61.255.55
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     *        *        *     请求超时。
 19     *        *        *     请求超时。
 20    45 ms    29 ms    33 ms  182.61.200.6

跟踪完成。
```



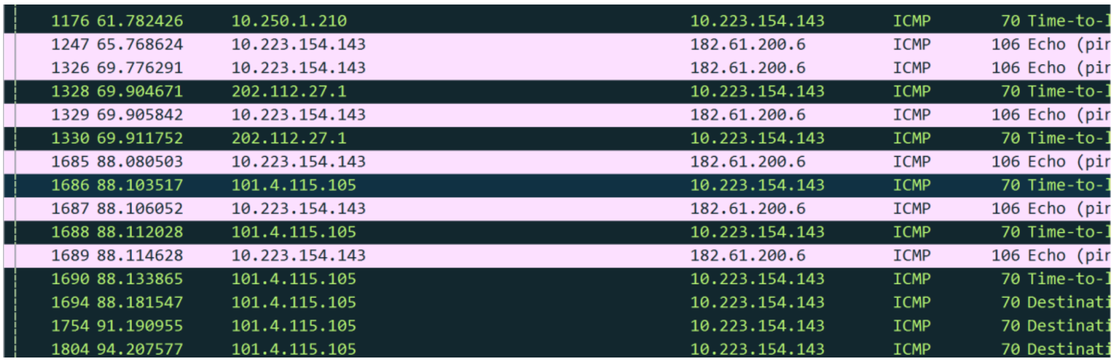
```
 56 3.452989    10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
109 7.272285    10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
219 11.272136   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
273 15.277673   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
274 15.291836   10.250.1.210      10.223.154.143    ICMP    70 Time-to-
275 15.292829   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
276 15.307383   10.250.1.210      10.223.154.143    ICMP    70 Time-to-
277 15.308475   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
278 15.332438   10.250.1.210      10.223.154.143    ICMP    70 Time-to-
287 15.493813   10.250.1.210      10.223.154.143    ICMP    70 Destinat
349 18.457817   10.250.1.210      10.223.154.143    ICMP    70 Destinat
390 21.470857   10.250.1.210      10.223.154.143    ICMP    70 Destinat
504 25.461014   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
505 25.467716   10.250.1.214      10.223.154.143    ICMP    70 Time-to-
506 25.468551   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
512 25.479443   10.250.1.214      10.223.154.143    ICMP    70 Time-to-
513 25.480328   10.223.154.143    182.61.200.6      ICMP   106 Echo (pi
```



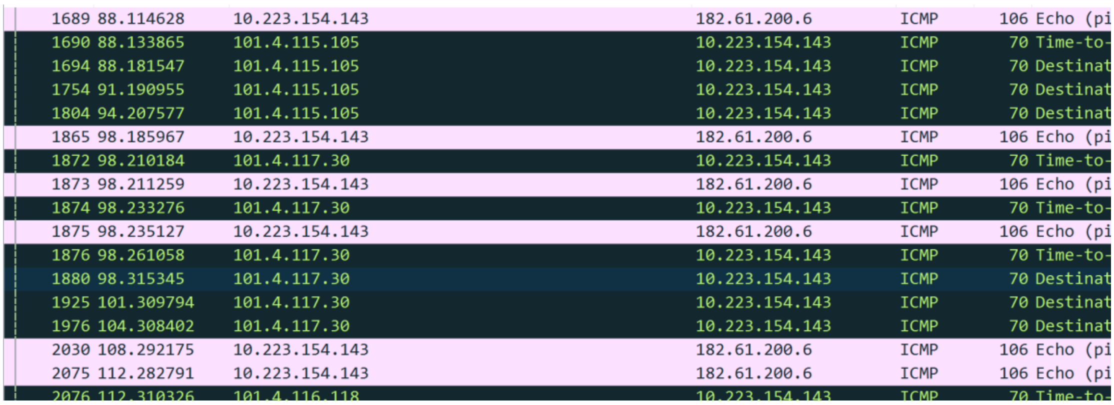
```
 519 25.527835   10.250.1.214      10.223.154.143  ICMP   70 Time-to-
 525 25.543579   10.250.1.214      10.223.154.143  ICMP   70 Destinat
 632 28.550908   10.250.1.214      10.223.154.143  ICMP   70 Destinat
 679 31.554352   10.250.1.214      10.223.154.143  ICMP   70 Destinat
 724 35.525059   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
 726 35.534709   10.255.19.1       10.223.154.143  ICMP  110 Time-to-
 727 35.536406   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
 728 35.538429   10.255.19.1       10.223.154.143  ICMP  110 Time-to-
 729 35.539810   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
 730 35.542958   10.255.19.1       10.223.154.143  ICMP  110 Time-to-
 734 35.582331   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
 784 38.574245   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
 822 41.588826   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
 885 45.598391   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
 886 45.600691   10.255.249.45     10.223.154.143  ICMP  110 Time-to-
```



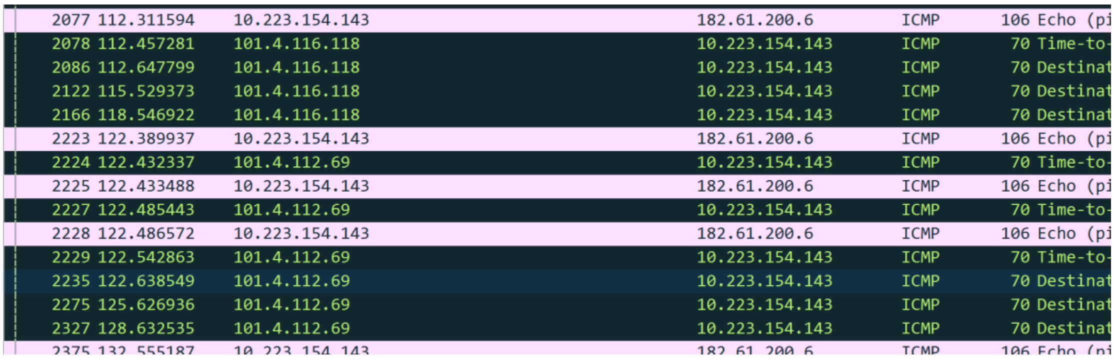
```
 886 45.600691   10.255.249.45     10.223.154.143  ICMP  110 Time-to-
 887 45.601670   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
 888 45.608282   10.255.249.45     10.223.154.143  ICMP  110 Time-to-
 889 45.609192   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
 890 45.612153   10.255.249.45     10.223.154.143  ICMP  110 Time-to-
 894 45.638419   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
 938 48.641394   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
 985 51.641612   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
1045 55.659772   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1046 55.673724   10.255.38.250     10.223.154.143  ICMP   70 Time-to-
1047 55.675067   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1048 55.693065   10.255.38.250     10.223.154.143  ICMP   70 Time-to-
1049 55.694240   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1051 55.717106   10.255.38.250     10.223.154.143  ICMP   70 Time-to-
1056 55.892309   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
1106 58.772265   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
```



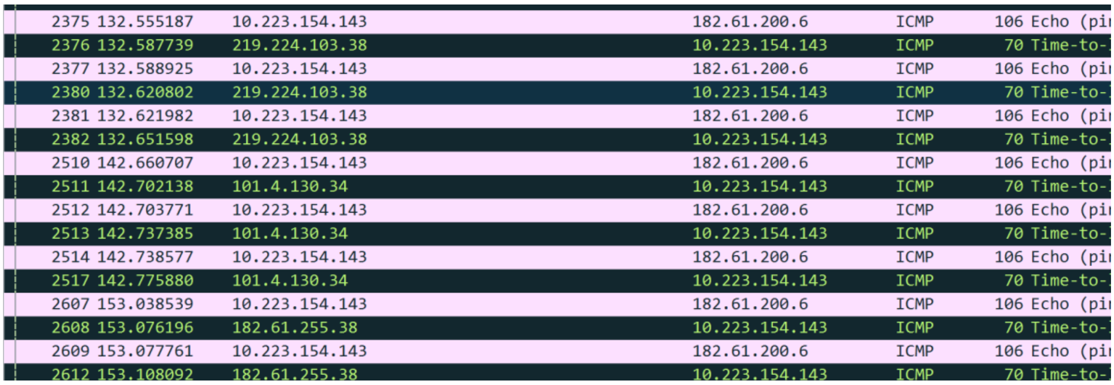
```
1176 61.782426   10.250.1.210      10.223.154.143  ICMP   70 Time-to-
1247 65.768624   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1326 69.776291   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1328 69.904671   202.112.27.1      10.223.154.143  ICMP   70 Time-to-
1329 69.905842   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1330 69.911752   202.112.27.1      10.223.154.143  ICMP   70 Time-to-
1685 88.080503   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1686 88.103517   101.4.115.105     10.223.154.143  ICMP   70 Time-to-
1687 88.106052   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1688 88.112028   101.4.115.105     10.223.154.143  ICMP   70 Time-to-
1689 88.114628   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1690 88.133865   101.4.115.105     10.223.154.143  ICMP   70 Time-to-
1694 88.181547   101.4.115.105     10.223.154.143  ICMP   70 Destinat
1754 91.190955   101.4.115.105     10.223.154.143  ICMP   70 Destinat
1804 94.207577   101.4.115.105     10.223.154.143  ICMP   70 Destinat
```



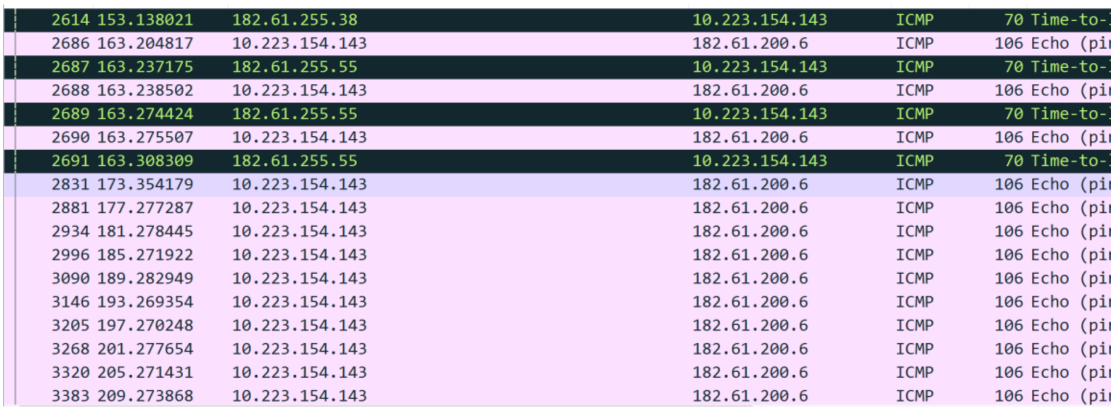
```
1689 88.114628   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1690 88.133865   101.4.115.105     10.223.154.143  ICMP   70 Time-to-
1694 88.181547   101.4.115.105     10.223.154.143  ICMP   70 Destinat
1754 91.190955   101.4.115.105     10.223.154.143  ICMP   70 Destinat
1804 94.207577   101.4.115.105     10.223.154.143  ICMP   70 Destinat
1865 98.185967   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1872 98.210184   101.4.117.30      10.223.154.143  ICMP   70 Time-to-
1873 98.211259   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1874 98.233276   101.4.117.30      10.223.154.143  ICMP   70 Time-to-
1875 98.235127   10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
1876 98.261058   101.4.117.30      10.223.154.143  ICMP   70 Time-to-
1880 98.315345   101.4.117.30      10.223.154.143  ICMP   70 Destinat
1925 101.309794  101.4.117.30      10.223.154.143  ICMP   70 Destinat
1976 104.308402  101.4.117.30      10.223.154.143  ICMP   70 Destinat
2030 108.292175  10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
2075 112.282791  10.223.154.143    182.61.200.6    ICMP  106 Echo (pi
2076 112.310326  101.4.116.118     10.223.154.143  ICMP   70 Time-to-
```



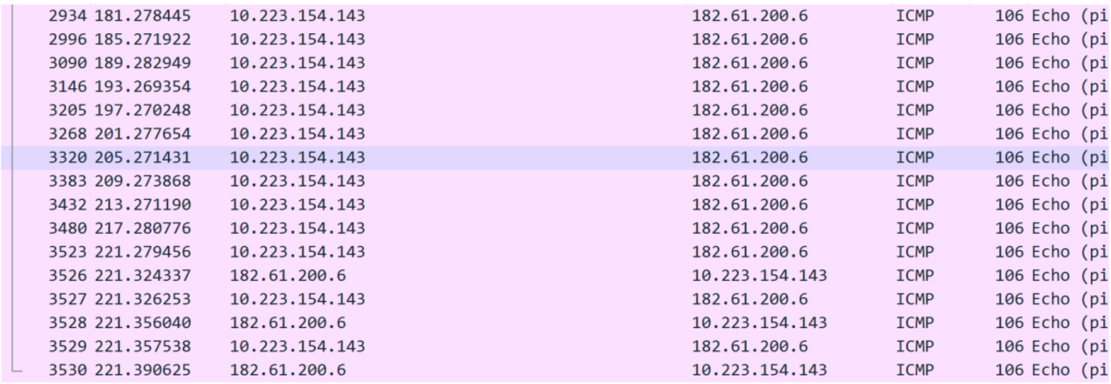
```
2077 112.311594   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2078 112.457281   101.4.116.118         10.223.154.143   ICMP     70 Time-to-
2086 112.647799   101.4.116.118         10.223.154.143   ICMP     70 Destinat
2122 115.529373   101.4.116.118         10.223.154.143   ICMP     70 Destinat
2166 118.546922   101.4.116.118         10.223.154.143   ICMP     70 Destinat
2223 122.389937   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2224 122.432337   101.4.112.69          10.223.154.143   ICMP     70 Time-to-
2225 122.433488   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2227 122.485443   101.4.112.69          10.223.154.143   ICMP     70 Time-to-
2228 122.486572   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2229 122.542863   101.4.112.69          10.223.154.143   ICMP     70 Time-to-
2235 122.638549   101.4.112.69          10.223.154.143   ICMP     70 Destinat
2275 125.626936   101.4.112.69          10.223.154.143   ICMP     70 Destinat
2327 128.632535   101.4.112.69          10.223.154.143   ICMP     70 Destinat
2375 132.555187   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
```



```
2375 132.555187   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2376 132.587739   219.224.103.38        10.223.154.143   ICMP     70 Time-to-
2377 132.588925   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2380 132.620802   219.224.103.38        10.223.154.143   ICMP     70 Time-to-
2381 132.621982   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2382 132.651598   219.224.103.38        10.223.154.143   ICMP     70 Time-to-
2510 142.660707   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2511 142.702138   101.4.130.34          10.223.154.143   ICMP     70 Time-to-
2512 142.703771   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2513 142.737385   101.4.130.34          10.223.154.143   ICMP     70 Time-to-
2514 142.738577   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2517 142.775880   101.4.130.34          10.223.154.143   ICMP     70 Time-to-
2607 153.038539   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2608 153.076196   182.61.255.38         10.223.154.143   ICMP     70 Time-to-
2609 153.077761   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2612 153.108092   182.61.255.38         10.223.154.143   ICMP     70 Time-to-
```



```
2614 153.138021   182.61.255.38         10.223.154.143   ICMP     70 Time-to-
2686 163.204817   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2687 163.237175   182.61.255.55         10.223.154.143   ICMP     70 Time-to-
2688 163.238502   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2689 163.274424   182.61.255.55         10.223.154.143   ICMP     70 Time-to-
2690 163.275507   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2691 163.308309   182.61.255.55         10.223.154.143   ICMP     70 Time-to-
2831 173.354179   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2881 177.277287   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2934 181.278445   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2996 185.271922   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3090 189.282949   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3146 193.269354   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3205 197.270248   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3268 201.277654   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3320 205.271431   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3383 209.273868   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
```



```
2934 181.278445   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
2996 185.271922   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3090 189.282949   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3146 193.269354   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3205 197.270248   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3268 201.277654   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3320 205.271431   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3383 209.273868   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3432 213.271190   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3480 217.280776   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3523 221.279456   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3526 221.324337   182.61.200.6          10.223.154.143   ICMP    106 Echo (pi
3527 221.326253   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3528 221.356040   182.61.200.6          10.223.154.143   ICMP    106 Echo (pi
3529 221.357538   10.223.154.143        182.61.200.6     ICMP    106 Echo (pi
3530 221.390625   182.61.200.6          10.223.154.143   ICMP    106 Echo (pi
```

Traceroute 的工作原理:基本的原理是 IP 路由过程中对 UDP 数据包 TTL(Time to Live，存活时间)的处理。当路由器收到一个 IP 包时，会减小 IP 包的 TTL。每收到一个包，检查这个 的 TTL 是否是 0 或 1。假设是，表明这个包还没有到达目的地，并且剩余时间不多了，肯定是到不了目的地了。这样路由器就简单地丢弃这个包，并给源主机发送 ICMP 通知，说这个包已经超时了。ICMP 的通知信息

里包括当前路由器发送时所用的 IP。那么主机一开始发送一个 TTL=1 的包，这样第一个包就会发现超时，由此得到第一个包的 IP，再发送一个 TTL=2 的包以此类推得知道数据包可以传送到目标主机。这样所有从源主机到目标主机所经过的路由都会被检测到。