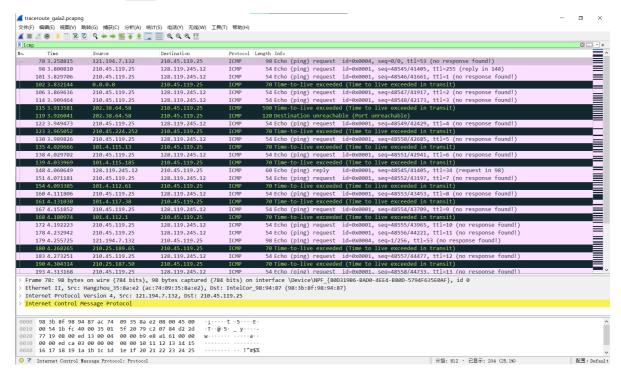
PW2 实验文档

实验名称: traceroute

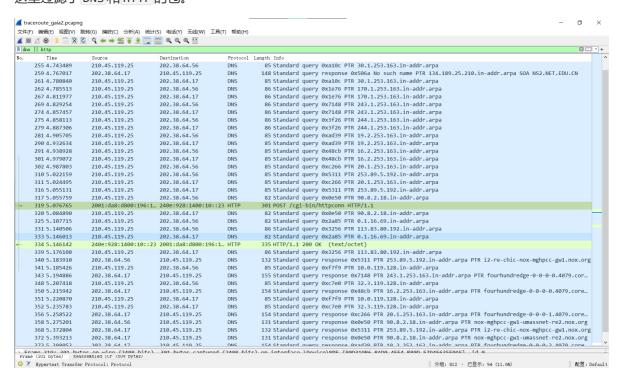
A1

1. 过滤得到所有 ICMP 包的结果:



2. 过滤得到其他应用层协议包的结果:

这里过滤了 DNS 和 HTTP 的包。



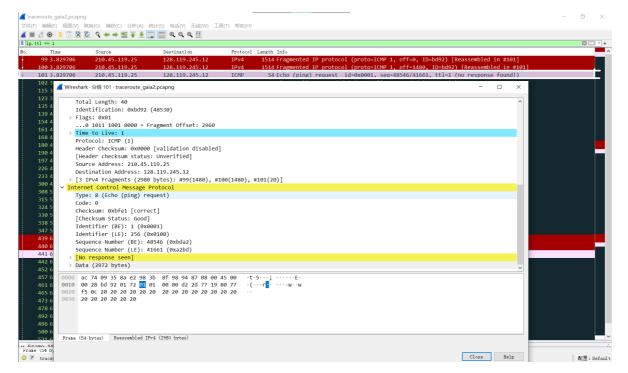
HTTP 的包应该不是 traceroute 产生的,因为我另一次 traceroute 时抓到的 HTTP 与Windows自动更新有关;我一个同学抓的包里就没有 HTTP 包。

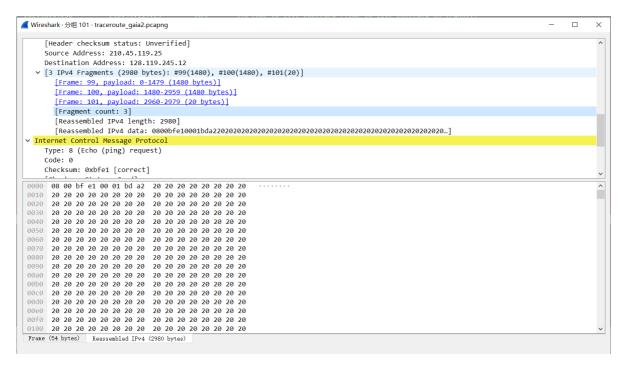
A2

1. 从本机到 gaia.cs.umas.edu 主机, 一共有36跳:

```
通过最多 48 个跃点跟踪
到 gaia.cs.umass.edu [128.119.245.12] 的路由:
                  34 ms
                            17 ms 202.141.164.254
                                    请求超时。
10.12.2.53
  2
        *
       22 ms
                  18 ms
                            20 ms
  3
  4
       27 ms
                            16 ms
                  19 ms
                                    61.190.195.53
       13 ms
                  18 ms
                                    61.191.109.201
  6
       50 ms
                  61 ms
                            38 ms
                                    202.102.205.77
  7
       21 ms
                  40 ms
                            23 ms 202.97.100.5
  8
                   *
                             *
                                    请求超时。
  9
                                    请求超时。
 10
      162 ms
                 172 ms
                           157 ms
                                    202.97.51.206
                 158 ms
      238 ms
                                    be-221-pe04.9greatoaks.ca.ibone.comcast.net [66.208.216.33]
 11
                           161 ms
                 204 ms
                           204 ms
                                    be-2204-cs02.9greatoaks.ca.ibone.comcast.net [96.110.36.181]
be-1212-cr12.9greatoaks.ca.ibone.comcast.net [68.86.166.146]
 12
      237 ms
 13
      221 ms
                 400 ms
                           202 ms
                                    be-301-cr12.sunnyvale.ca.ibone.comcast.net [96.110.37.169]
 14
      202 ms
                 307 ms
                           203 ms
                                    be-1312-cs03.sunnyvale.ca.ibone.comcast.net [96.110.46.29]
be-1311-cr11.sunnyvale.ca.ibone.comcast.net [96.110.46.26]
      164 ms
 15
                 239 ms
                           205 ms
 16
      168 ms
                 228 ms
      180 ms
                 179 ms
                           193 ms
                                    be-304-cr12.champa.co.ibone.comcast.net [96.110.39.29]
 17
                                    be-1412-cs04.champa.co.ibone.comcast.net [96.110.37.221]
be-1413-cr13.champa.co.ibone.comcast.net [96.110.37.238]
 18
      206 ms
                 195 ms
                           204 ms
                 295 ms
 19
      305 ms
                           210 ms
                 204 ms
                           203 ms
                                    be-302-cr13.1601milehigh.co.ibone.comcast.net [96.110.36.198]
 20
      209 ms
                                    be-1413-cs04.1601milehigh.co.ibone.comcast.net [96.110.39.109]
be-1411-cr11.1601milehigh.co.ibone.comcast.net [96.110.39.78]
 21
      297 ms
                 302 ms
                           304 ms
 22
      175 ms
                 245 ms
        *
                  *
                             *
                                    请求超时。
      331 ms
 24
                 317 ms
                           221 ms
                                    be-1111-cs01.350ecermak.il.ibone.comcast.net [96.110.35.1]
                 249 ms
                           361 ms
                                    be-1112-cr12.350ecermak.il.ibone.comcast.net [96.110.35.18]
 25
      296 ms
 26
      267 ms
                           289 ms
                                    be-301-cr11.newyork.ny.ibone.comcast.net [96.110.38.66]
                 212 ms
                                    be-1111-cs01.newyork.ny.ibone.comcast.net [96.110.35.113]
 27
      335 ms
                 258 ms
                           218 ms
 28
      223 ms
                 223 ms
                           265 ms
                                    be-32011-ar01.needham.ma.boston.comcast.net [96.110.42.2]
 29
      263 ms
                                    162.151.53.214
                 300 ms
                           220 ms
                                    96.108.44.226
 30
      300 ms
                 240 ms
                           269 ms
                                    请求超时。
 31
                  *
                             *
 32
      248 ms
                 321 ms
                           307 ms
                                    core2-rt-et-8-3-0.gw.umass.edu [192.80.83.113]
                                    n5-rt-1-1-et-10-0-0.gw.umass.edu [128.119.0.10]
 33
      255 ms
                 276 ms
                           285 ms
      289 ms
                                    cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
 34
                 278 ms
                           256 ms
                                    nscs1bbs1.cs.umass.edu [128.119.240.253]
      343 ms
 35
                 306 ms
                           306 ms
                                    gaia.cs.umass.edu [128.119.245.12]
 36
      284 ms
                 306 ms
                           223 ms
跟踪完成。
```

2. 下图为 ICMP 第一个ttl = 1的 Echo Request 的包:





一共分了3片。 (Fragment count: 3)

分片是因为,我们在设置里把包的大小设为3000 Bytes,并且允许包的分片;MTU最大是1500 Bytes,除去各协议的头部,小于包的长度,所以会分片。

A3

- 1. fregamentation and reassembly: IP报文被分片后,只在dst_host处重组;报文的每个分片的小报文里,携带报文长度、ID (同个大报文的片段拥有同个ID)、flag (标识是否是最后一个报文片段,若flag=0x1,则不是,若flag=0x0,则是)和offset (表示该报文片段位于大报文的哪个位置)
- 2. 如下图的两个fregment就分别是中间和最后一个报文片段:

```
ip. dst_host == 128.119.245.12 && ip. flags == 0x1

■ Wireshark · 分组 101 · traceroute_gaia2.pcapng

 > Frame 101: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF
 > Ethernet II, Src: IntelCor_98:94:87 (98:3b:8f:98:94:87), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:
 ✓ Internet Protocol Version 4, Src: 210.45.119.25, 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: 40
      Identification: 0xbd92 (48530)
    > Flags: 0x01
      ...0 1011 1001 0000 = Fragment Offset: 2960
    > Time to Live: 1
      Protocol: ICMP (1)
      Header Checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
  0000 ac 74 09 35 8a e2 98 3b 8f 98 94 87 08 00 45 00 0010 00 28 bd 92 01 72 01 01 00 00 d2 2d 77 19 80 77
                                                            ·t·5...; ·····E·
                                                            ·(···r···-w··w
  0030 20 20 20 20 20 20
  Frame (54 bytes) Reassembled IPv4 (2980 bytes)
```

上图是报文片段的中间部分。

```
| ip. dst_host == 128.119.245.12 && ip.flags == 0x0

■ Wireshark・分组 115・traceroute gaia2.pcapng

 > Frame 115: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\N
 > Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_98:94:87 (98:3b:8f:98:94
 v Internet Protocol Version 4, Src: 202.38.64.58, Dst: 210.45.119.25
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
   Total Length: 576
    Identification: 0xd486 (54406)
  > Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 62
    Protocol: ICMP (1)
    Header Checksum: 0x51cf [validation disabled]
    [Hoodon chackeum status: Unvanified]
 0010 02 40 d4 86 00 00 3e 01 51 cf ca 26 40 3a d2 2d
                                   ·@····>· Q··&@:·-
 0020 77 19 0b 00 ce d9 00 00 00 00 45 00 05 dc bd 94
                                   W - - - - - - - - - F - - - - -
 0030 20 00 01 01 17 c2 d2 2d 77 19 80 77 f5 0c 08 00
                                   · · · · · - W · · W · · · ·
 0040 bf df 00 01 bd a4 20 20 20 20 20 20 20 20 20 20
```

上图是报文片段的结尾(最后一个片段)。

3. Total Length 表示这个报文片段的长度:

```
— Wireshark · 分组 101 · traceroute_gaia2.pcapng

 > Frame 101: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface
 > Ethernet II, Src: IntelCor_98:94:87 (98:3b:8f:98:94:87), Dst: Hangzhou_35:8a:e2
✓ Internet Protocol Version 4, Src: 210.45.119.25, 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: 40
     Identification: 0xbd92 (48530)
   > Flags: 0x01
     ...0 1011 1001 0000 = Fragment Offset: 2960
   > Time to Live: 1
     Protocol: ICMP (1)
     Header Checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
 0000 ac 74 09 35 8a e2 98 3b 8f 98 94 87 08 00 45 00
                                                       ·t·5···; ·····E·
 0010 00 28 bd 92 01 72 01 01 00 00 d2 2d 77 19 80 77
                                                       ·(···r·· ···-w··w
 0030 20 20 20 20 20 20
 Frame (54 bytes) Reassembled IPv4 (2980 bytes)
```

上图表示该报文片段的长度为40 bytes。

A4

如图,ttl-exceeded包会返回给路由器,payload里有Type: 11的字段(Time-to-live exceeded)。

```
文件(E) 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(I) 帮助(H)
ip. ttl
           Time
                             Source
                                                       Destination
                                                                                 Protocol Length Info
                            210.45.119.25
                                                      51.132.193.104
       60 2.684591
                                                                                               55 60316 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reass
       66 3,006897
                            51,132,193,104
                                                      210.45.119.25
                                                                                 TCP
                                                                                               66 443 → 60316 [ACK] Seg=1 Ack=2 Win=2049 Len=0 SLE=1 SRE=2
       69 3.154277
                                                                                               77 Standard query 0x12d9 A gaia.cs.umass.edu
                            210.45.119.25
                                                      202.38.64.56
                                                                                 DNS
       70 3.154557
                            210.45.119.25
                                                      202.38.64.56
                                                                                 DNS
                                                                                               77 Standard query 0x91f7 AAAA gaia.cs.umass.edu
                                                      210.45.119.25
                                                                                              130 Standard query response 0x91f7 AAAA gaia.cs.umass.edu SOA unix1.cs.
       76 3.181635
                            202.38.64.56
                                                                                 DNS
        77 3.186575
                            210.45.119.25
                                                       202.38.64.17
                                                                                               77 Standard query 0x12d9 A gaia.cs.umass.edu
                                                                                 DNS
                                                                                                98 Echo (ping) request id=0x0004, seq=0/0, ttl=53 (no response found
        78 3.258815
                                                       210.45.119.25
                                                                                 ICMP
                            121.194.7.132
        82 3.384919
                            210.45.119.25
                                                       20.150.43.132
                                                                                                54 60283 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=
                                                                                               60 443 → 60283 [FIN, ACK] Seq=1 Ack=2 Win=2048 Len=0
54 60283 → 443 [ACK] Seq=2 Ack=2 Win=515 Len=0
       88 3,628613
                            20.150.43.132
                                                      210.45.119.25
                                                                                 TCP
                                                                                 TCP
       90 3,646084
                            202.38.64.17
                                                      210.45.119.25
                                                                                 DNS
                                                                                               93 Standard query response 0x12d9 A gaia.cs.umass.edu A 128.119.245.12
        94 3,784630
                            202.38.96.55
                                                       255,255,255,255
                                                                                                                      Transaction ID 0x6bd56ea2
                                                                                             93 Standard query response 0x12d9 A gaia.cs.umass.edu A 128.119.245.12
1514 Fragmented IP protocol (proto=ICMP 1, off=0, ID=bd91) [Reassembled
       95 3.790476
                            202.38.64.56
                                                       210.45.119.25
                                                                                 DNS
        96 3.800810
                            210.45.119.25
                                                       128.119.245.12
                                                                                 IPv4
                                                       128.119.245.12
       97 3.800810
                            210.45.119.25
                                                                                 TPv4
                                                                                             1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=bd91) [Reassembl
       98 3.800810
                            210.45.119.25
                                                      128.119.245.12
                                                                                 ICMP
                                                                                               54 Echo (ping) request id=0x0001, seq=48545/41405, ttl=255 (reply in
                                                                                             1514 Fragmented IP protocol (proto=ICMP 1, off=e, ID=bd92) [Reassembled 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=bd92) [Reassembled 1514 Fragmented IP protocol (proto=ICMP 1, off=1480, ID=bd92) [Reassemble 54 Echo (ping) request id=0x0001, seq=48546/41661, ttl=1 (no respons 70 Time-to-live exceeded (Time to live exceeded in teamsit)
                            210.45.119.25
210.45.119.25
      100 3.829706
                                                       128,119,245,12
                                                                                 TPv4
      102 3.832144
                           0.0.0.0
                                                      210.45.119.25

■ Wireshark · 分组 102 · traceroute gaia2.pcapng

       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: 210.45.119.25, Dst: 128.119.245.12
      Internet Control Message Protocol
 0000 98 3b 8f 98 94 87 ac 74 09 35 8a e2 08 00 45 00 0010 00 38 75 96 00 00 ff 01 fc e7 00 00 00 00 d2 2d 0020 77 19 31 00 6f 7a 60 00 00 00 61 00 05 00 05 db d9 20 0030 20 00 01 01 17 c4 d2 2d 77 19 80 77 f5 0c 08 00
                                                                        w · · · oz · · · · E · · · · ·
  0040 bf e1 00 01 bd a2
```

A5

```
通过最多 48 个跃点跟踪
到 gaia.cs.umass.edu [128.119.245.12] 的路由:
                          17 ms 202.141.164.254
                34 ms
       24 ms
 1
                                  请求超时。
        *
                 *
                           *
  3
       22 ms
                18 ms
                          20 ms
                                 10.12.2.53
 4
                19 ms
       27 ms
                          16 ms
                                 61.190.195.53
       13 ms
 5
                18 ms
                                  61.191.109.201
                          38 ms
       50 ms
                61 ms
                                  202.102.205.77
  7
       21 ms
                40 ms
                          23 ms
                                  202.97.100.5
                                  请求超时。
 8
 9
                                  请求超时。
                  *
 10
      162 ms
               172 ms
                         157 ms
                                  202.97.51.206
               158 ms
      238 ms
                         161 ms
                                  be-221-pe04.9greatoaks.ca.ibone.comcast.net [66.208.216.33]
 12
      237 ms
               204 ms
                         204 ms
                                  be-2204-cs02.9greatoaks.ca.ibone.comcast.net [96.110.36.181]
               400 ms
                                  be-1212-cr12.9greatoaks.ca.ibone.comcast.net [68.86.166.146]
 13
      221 ms
                         202 ms
                                 be-301-cr12.sunnyvale.ca.ibone.comcast.net [96.110.37.169]
 14
      202 ms
               307 ms
                         203 ms
                         205 ms
                                  be-1312-cs03.sunnyvale.ca.ibone.comcast.net [96.110.46.29]
be-1311-cr11.sunnyvale.ca.ibone.comcast.net [96.110.46.26]
 15
      164 ms
                239 ms
 16
      168 ms
               228 ms
                                  be-304-cr12.champa.co.ibone.comcast.net [96.110.39.29]
 17
      180 ms
               179 ms
                         193 ms
                                  be-1412-cs04.champa.co.ibone.comcast.net [96.110.37.221]
               195 ms
18
      206 ms
                         204 ms
 19
      305 ms
                295 ms
                         210 ms
                                  be-1413-cr13.champa.co.ibone.comcast.net [96.110.37.238]
                                  be-302-cr13.1601milehigh.co.ibone.comcast.net [96.110.36.198]
 20
      209 ms
                204 ms
                         203 ms
21
      297 ms
               302 ms
                                  be-1413-cs04.1601milehigh.co.ibone.comcast.net [96.110.39.109]
                         304 ms
                                  be-1411-cr11.1601milehigh.co.ibone.comcast.net [96.110.39.78]
      175 ms
               245 ms
                           *
 23
                                  请求超时。
 24
      331 ms
                317 ms
                         221 ms
                                  be-1111-cs01.350ecermak.il.ibone.comcast.net [96.110.35.1]
                                  be-1112-cr12.350ecermak.il.ibone.comcast.net [96.110.35.18]
 25
      296 ms
               249 ms
                         361 ms
                                  be-301-cr11.newyork.ny.ibone.comcast.net [96.110.38.66]
26
      267 ms
               212 ms
                         289 ms
                258 ms
                         218 ms
 27
      335 ms
                                  be-1111-cs01.newyork.ny.ibone.comcast.net [96.110.35.113]
 28
                         265 ms
      223 ms
                223 ms
                                  be-32011-ar01.needham.ma.boston.comcast.net [96.110.42.2]
 29
      263 ms
               300 ms
                                  162.151.53.214
                         220 ms
                                 96.108.44.226
 30
      300 ms
               240 ms
                         269 ms
 31
                                  请求超时。
                 *
                                 core2-rt-et-8-3-0.gw.umass.edu [192.80.83.113]
n5-rt-1-1-et-10-0-0.gw.umass.edu [128.119.0.10]
      248 ms
                         307 ms
 32
                321 ms
 33
      255 ms
               276 ms
                         285 ms
      289 ms
                                 cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
 34
               278 ms
                         256 ms
                                  nscs1bbs1.cs.umass.edu [128.119.240.253]
 35
      343 ms
                306 ms
                         306 ms
                                 gaia.cs.umass.edu [128.119.245.12]
 36
      284 ms
                306 ms
                         223 ms
跟踪完成。
```

上图为traceroute的各跳路由器,由图知,从第7到第10跳是跨过了太平洋电缆,因为RTT明显增多(增加了7倍),说明路程更远。

router addresses: 202.97.100.5~202.97.51.206

A6

第7跳的平均RTT:

$$RTT\ average_7 = (21 + 40 + 23)/3 = 28ms$$

第10跳的平均RTT:

$$RTT\ average_{10} = (162 + 172 + 157)/3 = 164ms$$

太平洋海底电缆的距离:

$$S\ pacific = [(164 - 28)/2] * 10^{-3} * 2 * 10^8 = 1.36 * 10^7 m$$