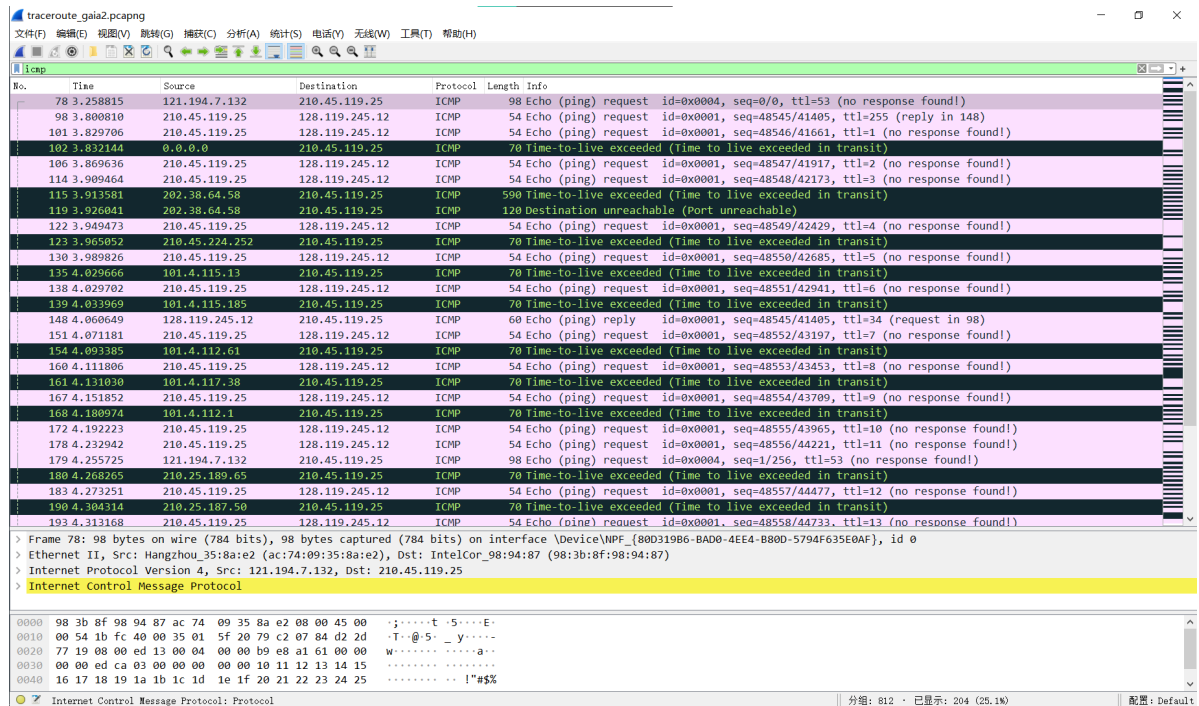


PW2 实验文档

实验名称: traceroute

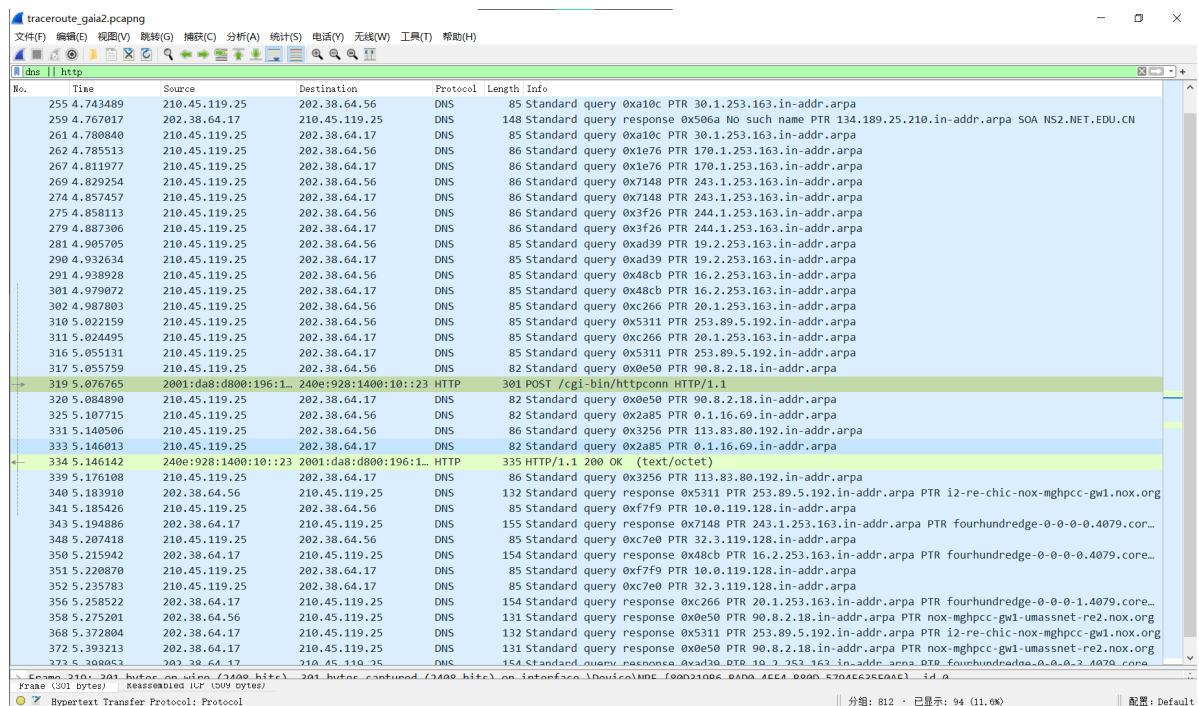
A1

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。

虽然上面这个截图里的 HTTP 包的链接打不开，但我合理推测，觉得和 traceroute 无关。

A2

1. 从本机到 gaia.cs.umass.edu 主机，一共有36跳：

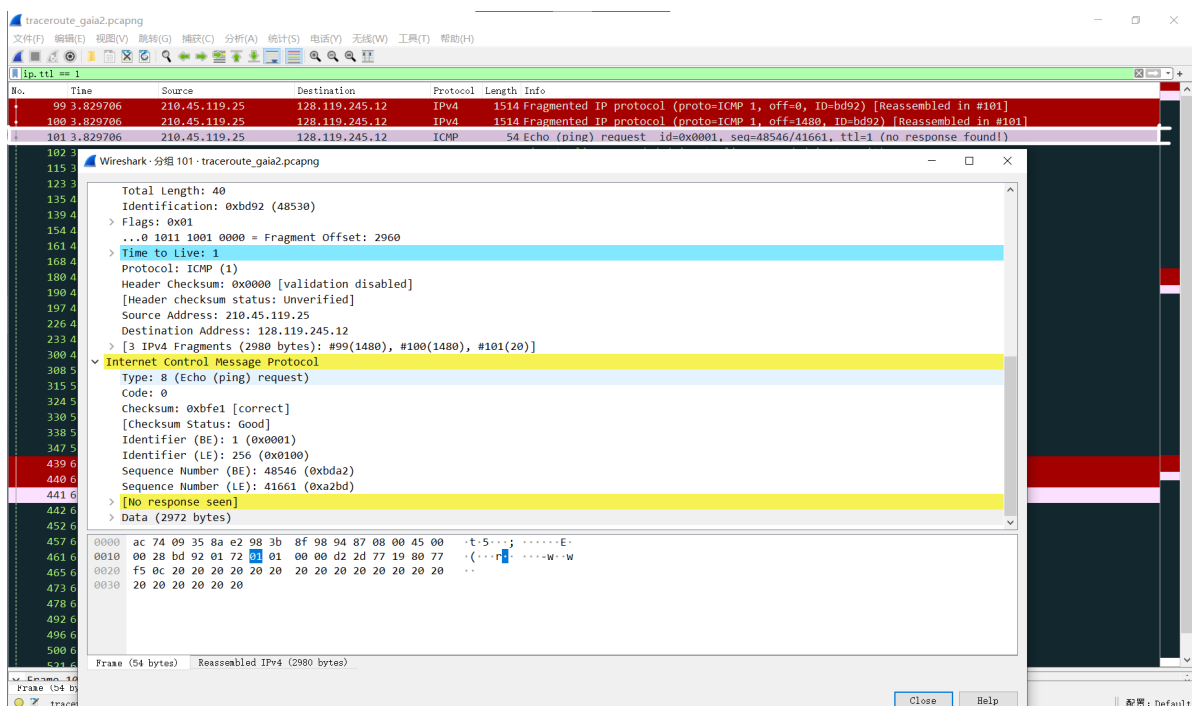
通过最多 48 个跃点跟踪

到 gaia.cs.umass.edu [128.119.245.12] 的路由：

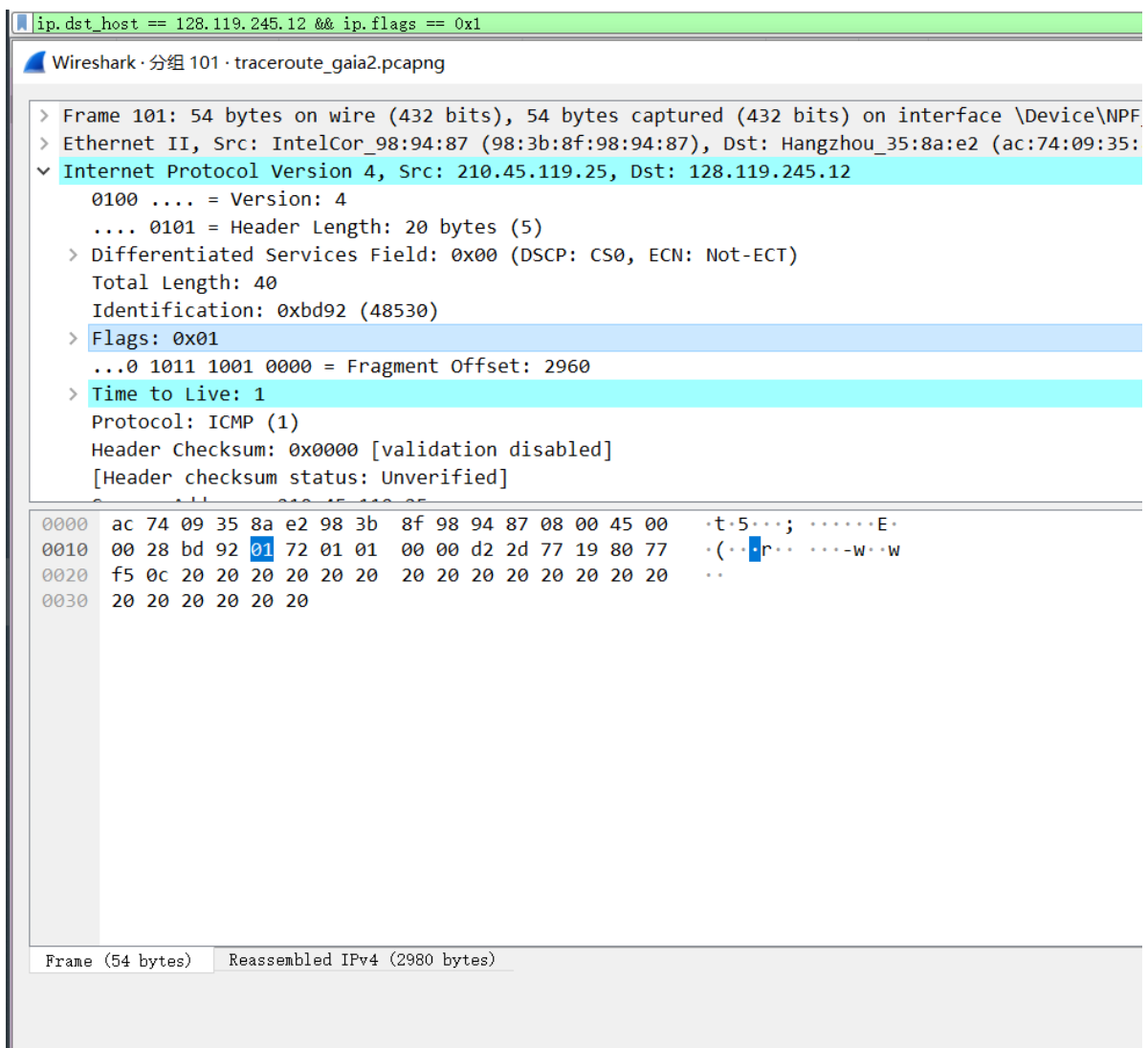
```
1    24 ms    34 ms    17 ms    202.141.164.254
2    *        *        *        请求超时。
3    22 ms    18 ms    20 ms    10.12.2.53
4    27 ms    19 ms    16 ms    61.190.195.53
5    13 ms    18 ms    *        61.191.109.201
6    50 ms    61 ms    38 ms    202.102.205.77
7    21 ms    40 ms    23 ms    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
11   238 ms   158 ms   161 ms   be-221-pe04.9greateoaks.ca.ibone.comcast.net [66.208.216.33]
12   237 ms   204 ms   204 ms   be-2204-cs02.9greateoaks.ca.ibone.comcast.net [96.110.36.181]
13   221 ms   400 ms   202 ms   be-1212-cr12.9greateoaks.ca.ibone.comcast.net [68.86.166.146]
14   202 ms   307 ms   203 ms   be-301-cr12.sunnyvale.ca.ibone.comcast.net [96.110.37.169]
15   164 ms   239 ms   205 ms   be-1312-cs03.sunnyvale.ca.ibone.comcast.net [96.110.46.29]
16   168 ms   228 ms   *        be-1311-cr11.sunnyvale.ca.ibone.comcast.net [96.110.46.26]
17   180 ms   179 ms   193 ms   be-304-cr12.champa.co.ibone.comcast.net [96.110.39.29]
18   206 ms   195 ms   204 ms   be-1412-cs04.champa.co.ibone.comcast.net [96.110.37.221]
19   305 ms   295 ms   210 ms   be-1413-cr13.champa.co.ibone.comcast.net [96.110.37.238]
20   209 ms   204 ms   203 ms   be-302-cr13.1601milehigh.co.ibone.comcast.net [96.110.36.198]
21   297 ms   302 ms   304 ms   be-1413-cs04.1601milehigh.co.ibone.comcast.net [96.110.39.109]
22   175 ms   245 ms   *        be-1411-cr11.1601milehigh.co.ibone.comcast.net [96.110.39.78]
23   *        *        *        请求超时。
24   331 ms   317 ms   221 ms   be-1111-cs01.350ecermak.il.ibone.comcast.net [96.110.35.1]
25   296 ms   249 ms   361 ms   be-1112-cr12.350ecermak.il.ibone.comcast.net [96.110.35.18]
26   267 ms   212 ms   289 ms   be-301-cr11.newyork.ny.ibone.comcast.net [96.110.38.66]
27   335 ms   258 ms   218 ms   be-1111-cs01.newyork.ny.ibone.comcast.net [96.110.35.113]
28   223 ms   223 ms   265 ms   be-32011-ar01.needham.ma.boston.comcast.net [96.110.42.2]
29   263 ms   300 ms   220 ms   162.151.53.214
30   300 ms   240 ms   269 ms   96.108.44.226
31   *        *        *        请求超时。
32   248 ms   321 ms   307 ms   core2-rt-et-8-3-0.gw.umass.edu [192.80.83.113]
33   255 ms   276 ms   285 ms   n5-rt-1-1-et-10-0-0.gw.umass.edu [128.119.0.10]
34   289 ms   278 ms   256 ms   cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
35   343 ms   306 ms   306 ms   nscs1bbs1.cs.umass.edu [128.119.240.253]
36   284 ms   306 ms   223 ms   gaia.cs.umass.edu [128.119.245.12]
```

跟踪完成。

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



3. 分片：



上图是报文片段的中间部分。

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

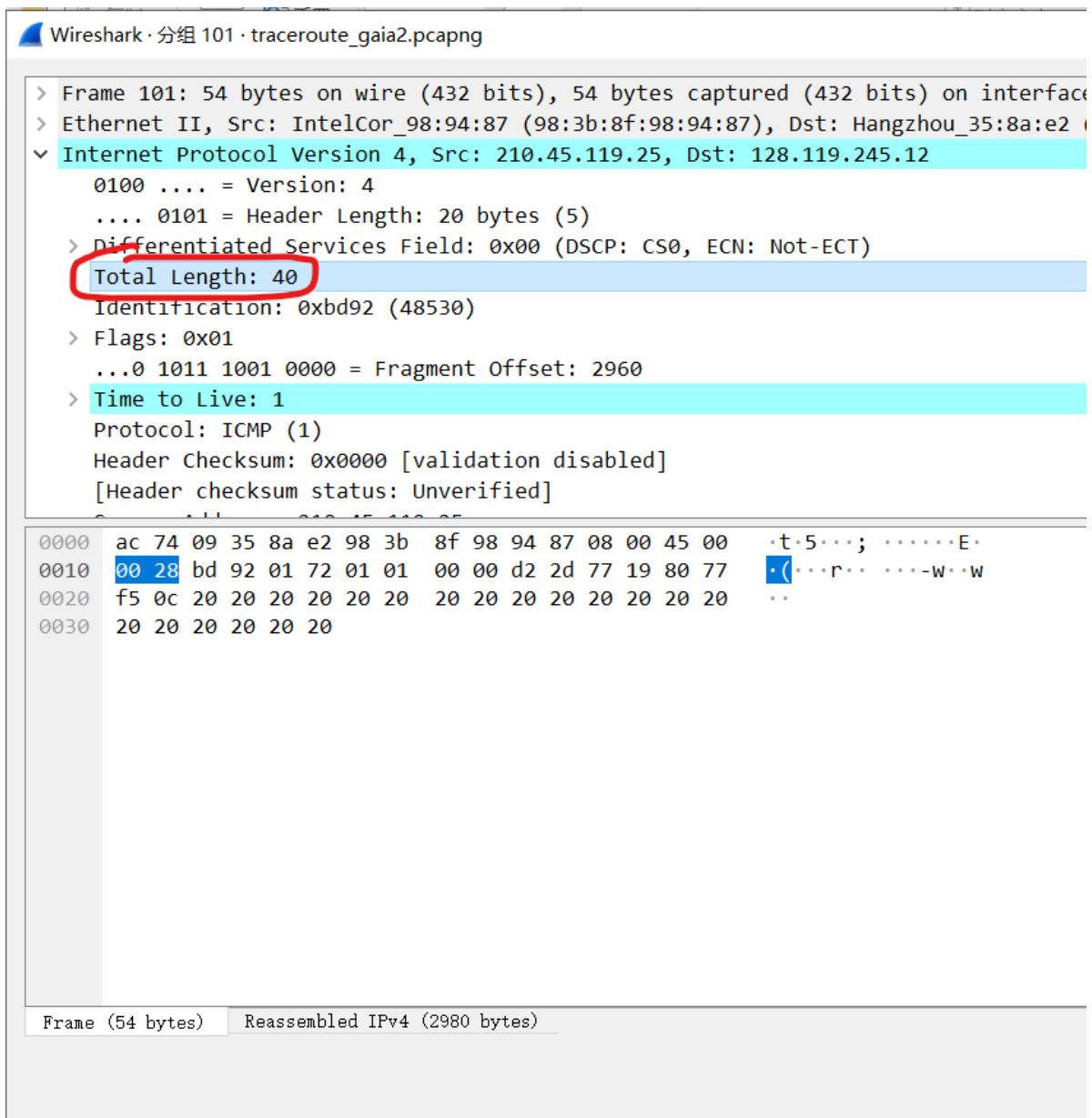
Wireshark · 分组 115 · traceroute_gaia2.pcapng

- > 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)
- ▼ 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]
 - [Header checksum status: Unverified]

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·········E·····
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	······
0050	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0060	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0070	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0080	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0090	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00a0	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00b0	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00c0	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00d0	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00e0	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
00f0	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0100	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0110	20 20 20 20 20 20 20 20 20 20 20 20 20 20	
0120	20 20 20 20 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：



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）。

tracert_gaia2.pcapng

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

ip.ttl

No.	Time	Source	Destination	Protocol	Length	Info
60	2.684591	210.45.119.25	51.132.193.104	TCP	55	60316 → 443 [ACK] Seq=1 Ack=1 Win=515 Len=1 [TCP segment of a reas
66	3.006897	51.132.193.104	210.45.119.25	TCP	66	443 → 60316 [ACK] Seq=1 Ack=2 Win=2049 Len=0 SLE=1 SRE=2
69	3.154277	210.45.119.25	202.38.64.56	DNS	77	Standard query 0x12d9 A gaia.cs.umass.edu
70	3.154557	210.45.119.25	202.38.64.56	DNS	77	Standard query 0x91f7 AAAA gaia.cs.umass.edu
76	3.181635	202.38.64.56	210.45.119.25	DNS	130	Standard query response 0x91f7 AAAA gaia.cs.umass.edu SOA unix1.cs.
77	3.186575	210.45.119.25	202.38.64.17	DNS	77	Standard query 0x12d9 A gaia.cs.umass.edu
78	3.258815	121.194.7.132	210.45.119.25	ICMP	98	Echo (ping) request id=0x0004, seq=0/0, ttl=53 (no response found!
82	3.384919	210.45.119.25	20.150.43.132	TCP	54	60283 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
88	3.628613	20.150.43.132	210.45.119.25	TCP	60	443 → 60283 [FIN, ACK] Seq=1 Ack=2 Win=2048 Len=0
89	3.628664	210.45.119.25	20.150.43.132	TCP	54	60283 → 443 [ACK] Seq=2 Ack=2 Win=515 Len=0
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	DHCP	342	DHCP NAK - Transaction ID 0x6bd56ea2
95	3.790476	202.38.64.56	210.45.119.25	DNS	93	Standard query response 0x12d9 A gaia.cs.umass.edu A 128.119.245.12
96	3.800810	210.45.119.25	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=bd91) [Reassembl
97	3.800810	210.45.119.25	128.119.245.12	IPv4	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
99	3.829706	210.45.119.25	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=bd92) [Reassembled
100	3.829706	210.45.119.25	128.119.245.12	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=bd92) [Reassembl
101	3.829706	210.45.119.25	128.119.245.12	ICMP	54	Echo (ping) request id=0x0001, seq=48546/41661, ttl=1 (no response
102	3.832144	0.0.0.0	210.45.119.25	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)

Wireshark - 分组 102: tracert_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 ;.....5....E
0010 00 38 75 96 00 00 ff 01 fc e7 00 00 00 d2 2d ;8u.....
0020 77 19 00 00 6f 7a 00 00 00 00 45 00 05 dc bd 92 W...oz....E....
0030 20 00 01 01 17 c4 d2 2d 77 19 80 77 f5 0c 08 00W..W....
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:

1	24 ms	34 ms	17 ms	202.141.164.254
2	*	*	*	请求超时。
3	22 ms	18 ms	20 ms	10.12.2.53
4	27 ms	19 ms	16 ms	61.190.195.53
5	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
11	238 ms	158 ms	161 ms	be-221-pe04.9greateaks.ca.ibone.comcast.net [66.208.216.33]
12	237 ms	204 ms	204 ms	be-2204-cs02.9greateaks.ca.ibone.comcast.net [96.110.36.181]
13	221 ms	400 ms	202 ms	be-1212-cr12.9greateaks.ca.ibone.comcast.net [68.86.166.146]
14	202 ms	307 ms	203 ms	be-301-cr12.sunnyvale.ca.ibone.comcast.net [96.110.37.169]
15	164 ms	239 ms	205 ms	be-1312-cs03.sunnyvale.ca.ibone.comcast.net [96.110.46.29]
16	168 ms	228 ms	*	be-1311-cr11.sunnyvale.ca.ibone.comcast.net [96.110.46.26]
17	180 ms	179 ms	193 ms	be-304-cr12.champa.co.ibone.comcast.net [96.110.39.29]
18	206 ms	195 ms	204 ms	be-1412-cs04.champa.co.ibone.comcast.net [96.110.37.221]
19	305 ms	295 ms	210 ms	be-1413-cr13.champa.co.ibone.comcast.net [96.110.37.238]
20	209 ms	204 ms	203 ms	be-302-cr13.1601milehigh.co.ibone.comcast.net [96.110.36.198]
21	297 ms	302 ms	304 ms	be-1413-cs04.1601milehigh.co.ibone.comcast.net [96.110.39.109]
22	175 ms	245 ms	*	be-1411-cr11.1601milehigh.co.ibone.comcast.net [96.110.39.78]
23	*	*	*	请求超时。
24	331 ms	317 ms	221 ms	be-1111-cs01.350ecermak.il.ibone.comcast.net [96.110.35.1]
25	296 ms	249 ms	361 ms	be-1112-cr12.350ecermak.il.ibone.comcast.net [96.110.35.18]
26	267 ms	212 ms	289 ms	be-301-cr11.newyork.ny.ibone.comcast.net [96.110.38.66]
27	335 ms	258 ms	218 ms	be-1111-cs01.newyork.ny.ibone.comcast.net [96.110.35.113]
28	223 ms	223 ms	265 ms	be-32011-ar01.needham.ma.boston.comcast.net [96.110.42.2]
29	263 ms	300 ms	220 ms	162.151.53.214
30	300 ms	240 ms	269 ms	96.108.44.226
31	*	*	*	请求超时。
32	248 ms	321 ms	307 ms	core2-rt-et-8-3-0.gw.umass.edu [192.80.83.113]
33	255 ms	276 ms	285 ms	n5-rt-1-1-et-10-0-0.gw.umass.edu [128.119.0.10]
34	289 ms	278 ms	256 ms	cics-rt-xe-0-0-0.gw.umass.edu [128.119.3.32]
35	343 ms	306 ms	306 ms	ns1cs1bbs1.cs.umass.edu [128.119.240.253]
36	284 ms	306 ms	223 ms	gaia.cs.umass.edu [128.119.245.12]

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:

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