利用 Wireshark 软件对微信协议的分析

——QPIC

贾冰杰　1120101251

全然　1120101259

王浩峰　1120101261　（组长）

谢青梅　1120101262

闫郡　1120101263

目录

一.实验规划：

1.接入手机,通过 wireshark 抓取微信数据包。

2.分析微信的登陆认证过程

3.分析微信的普通聊天过程

3.分析微信的典型应用——附近的人

4.总结：微信的协议

二. 实验内容：

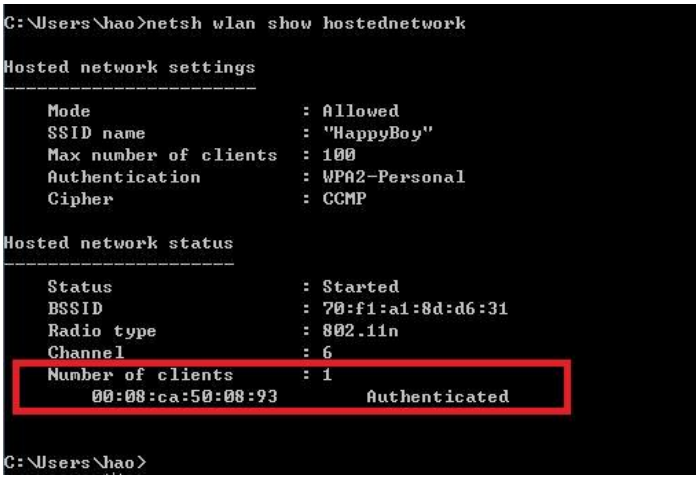
步骤 1、配置虚拟 AP：

由于微信的 pc 网页版本不容易操作，针对本次分析，我们使用 Android 手机系统下的微信客户端进行操作。通过手机连接至 pc 虚拟的无线网络进行微信的连接，这样通过 wireshark 软件进行抓包。

win7 系统下可以很容易将无线网卡设置为虚拟 AP,供其他无线设备接入。
配置脚本如下：

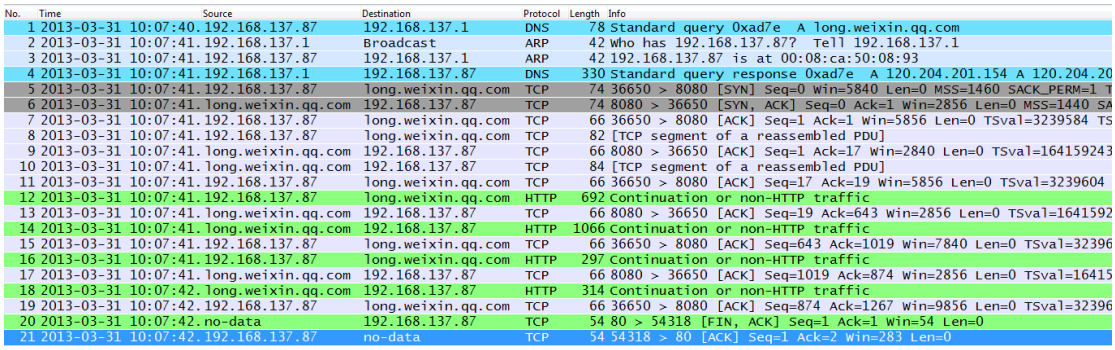
```
#Vitual_Wifi_setup.bat
netsh wlan set hostednetwork mode=allow ssid="HappyBoy" key=******
#在 GUI 界面下，将正在使用的某个网络连接共享给该虚拟 AP.
netsh wlan start hostednetwork
netsh wlan show hostednetwork
```

将手机接入后,可以看到: Number of clients 为 1.



打开 wireshark，能看到在接口列表中已经有虚拟 AP 了（如图）。手机接入后，打开微信 app，点击开始抓包，就能抓到微信数据包了。

步骤 2. 分析微信的登陆认证过程:



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-03-31 10:07:40.	192.168.137.87	192.168.137.1	DNS	78	Standard query 0xad7e A long.weixin.qq.com
2	2013-03-31 10:07:41.	192.168.137.1	Broadcast	ARP	42	Who has 192.168.137.87? Tell 192.168.137.1
3	2013-03-31 10:07:41.	192.168.137.87	192.168.137.1	ARP	42	192.168.137.87 is at 00:08:ca:50:08:93
4	2013-03-31 10:07:41.	192.168.137.1	192.168.137.87	DNS	330	Standard query response 0xad7e A 120.204.201.154 A 120.204.20
5	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	TCP	74	36650 > 8080 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 T
6	2013-03-31 10:07:41.	long.weixin.qq.com	192.168.137.87	TCP	74	8080 > 36650 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SA
7	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	TCP	66	36650 > 8080 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=3239584 TS
8	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	TCP	82	[TCP segment of a reassembled PDU]
9	2013-03-31 10:07:41.	long.weixin.qq.com	192.168.137.87	TCP	66	8080 > 36650 [ACK] Seq=1 Ack=17 Win=2840 Len=0 TSval=164159243
10	2013-03-31 10:07:41.	long.weixin.qq.com	192.168.137.87	TCP	84	[TCP segment of a reassembled PDU]
11	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	TCP	66	36650 > 8080 [ACK] Seq=17 Ack=19 Win=5856 Len=0 TSval=3239604
12	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	HTTP	692	Continuation or non-HTTP traffic
13	2013-03-31 10:07:41.	long.weixin.qq.com	192.168.137.87	TCP	66	8080 > 36650 [ACK] Seq=19 Ack=643 Win=2856 Len=0 TSval=1641592
14	2013-03-31 10:07:41.	long.weixin.qq.com	192.168.137.87	HTTP	1066	Continuation or non-HTTP traffic
15	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	TCP	66	36650 > 8080 [ACK] Seq=643 Ack=1019 Win=7840 Len=0 TSval=32396
16	2013-03-31 10:07:41.	192.168.137.87	long.weixin.qq.com	HTTP	297	Continuation or non-HTTP traffic
17	2013-03-31 10:07:41.	long.weixin.qq.com	192.168.137.87	TCP	66	8080 > 36650 [ACK] Seq=1019 Ack=874 Win=2856 Len=0 TSval=16415
18	2013-03-31 10:07:42.	long.weixin.qq.com	192.168.137.87	HTTP	314	Continuation or non-HTTP traffic
19	2013-03-31 10:07:42.	192.168.137.87	long.weixin.qq.com	TCP	66	36650 > 8080 [ACK] Seq=874 Ack=1267 Win=9856 Len=0 TSval=32396
20	2013-03-31 10:07:42.	no-data	192.168.137.87	TCP	54	80 > 54318 [FIN, ACK] Seq=1 Ack=1 Win=54 Len=0
21	2013-03-31 10:07:42.	192.168.137.87	no-data	TCP	54	54318 > 80 [ACK] Seq=1 Ack=2 Win=283 Len=0

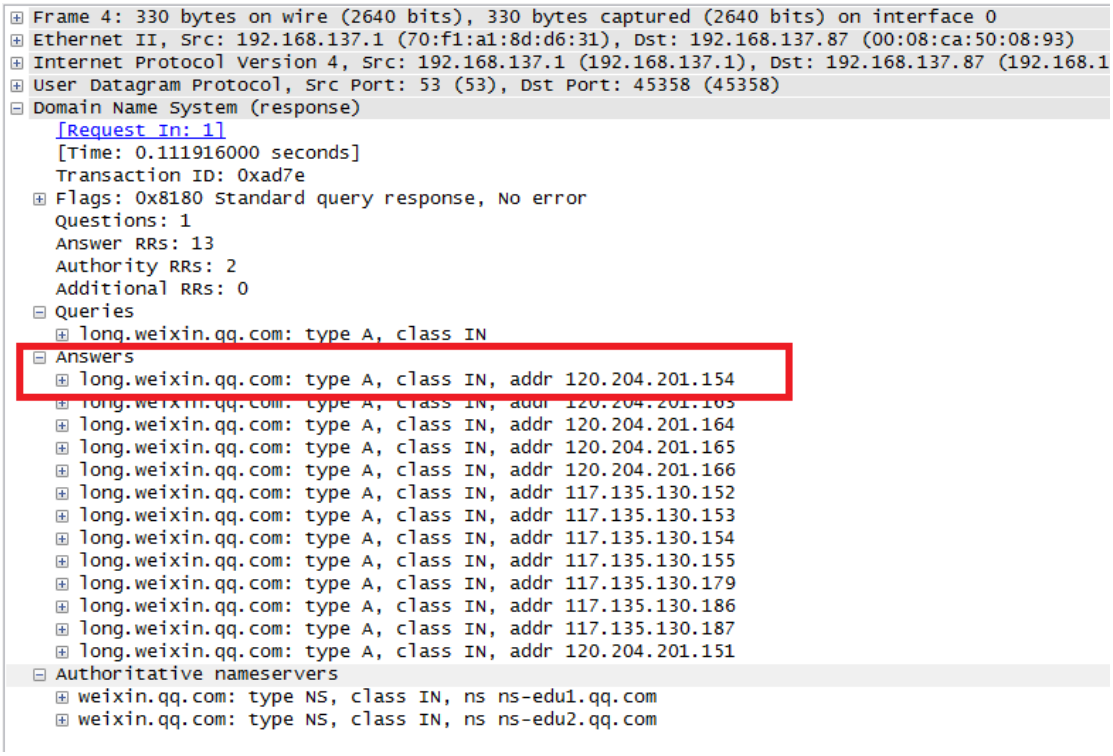
打开微信客户端，微信开始登录，可以看到手机分配到的 IP 为 192.168.137.87，AP 站点的 IP 为 192.168.137.1

第一包数据 是一个域名查询，微信客户端向网络查询微信服务器，域名为 long.weixin.qq.com 的 IP 地址；

第二包数据 是 ARP 地址解析，AP 站点向全网广播，询问 192.168.137.87 对应的 MAC 地址；

第三包数据 是 ARP 应答，手机告诉 AP 站点自己的 MAC 地址；

第四包数据 是第一包 DNS 查询的应答，将该包数据展开，可以看到：



```
⊞ Frame 4: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface 0
⊞ Ethernet II, Src: 192.168.137.1 (70:f1:a1:8d:d6:31), Dst: 192.168.137.87 (00:08:ca:50:08:93)
⊞ Internet Protocol Version 4, Src: 192.168.137.1 (192.168.137.1), Dst: 192.168.137.87 (192.168.1
⊞ User Datagram Protocol, Src Port: 53 (53), Dst Port: 45358 (45358)
⊟ Domain Name System (response)
    [Request In: 1]
    [Time: 0.111916000 seconds]
    Transaction ID: 0xad7e
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 13
    Authority RRs: 2
    Additional RRs: 0
  ⊟ Queries
    ⊞ long.weixin.qq.com: type A, class IN
  ⊟ Answers
    ⊞ long.weixin.qq.com: type A, class IN, addr 120.204.201.154
    ⊞ long.weixin.qq.com: type A, class IN, addr 120.204.201.163
    ⊞ long.weixin.qq.com: type A, class IN, addr 120.204.201.164
    ⊞ long.weixin.qq.com: type A, class IN, addr 120.204.201.165
    ⊞ long.weixin.qq.com: type A, class IN, addr 120.204.201.166
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.152
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.153
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.154
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.155
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.179
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.186
    ⊞ long.weixin.qq.com: type A, class IN, addr 117.135.130.187
    ⊞ long.weixin.qq.com: type A, class IN, addr 120.204.201.151
  ⊟ Authoritative nameservers
    ⊞ weixin.qq.com: type NS, class IN, ns ns-edu1.qq.com
    ⊞ weixin.qq.com: type NS, class IN, ns ns-edu2.qq.com
```

可以看到，查询到微信域名 long.weixin.qq.com 的多个服务器 IP。 接下来 TCP 的通信过程表明，微信客户端选择了 IP 为 120.204.201.154 的主机进行数据传送。

步骤 3. 分析微信的普通聊天过程

先是建立 TCP 连接：第 5 到第 7 包数据是 TCP 的三次握手

```
5 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   TCP   74 36650 > 8080 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3239570 TSecr=0 WS=32
6 2013-03-31 10:07:41.:120.204.201.154  192.168.137.87    TCP   74 8080 > 36650 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM=1 TSval=1641592389 TSe
7 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   TCP   66 36650 > 8080 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=3239584 TSecr=1641592389
```

首先客户端向服务器发送标志为 SYN 的连接请求，数据包标号 Seq=0；

```
TCP   74 36650 > 8080 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=3239570 TSecr=0 WS=32
TCP   74 8080 > 36650 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM=1 TSval=1641592389
TCP   66 36650 > 8080 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=3239584 TSecr=1641592389
```

收到请求后，服务器向客户端发送了带有 SYN 和 ACK 的确认应答，发送序号 Seq=0，确认序号 ACK=1；接下来，客户端向服务器发送确认应答，Seq=1，ACK=1. 连接建立完成。

```
 7 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   TCP    66 36650 > 8080 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=3239584 TSecr=1641592389
 8 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   TCP    82 [TCP segment of a reassembled PDU]
 9 2013-03-31 10:07:41.:120.204.201.154  192.168.137.87    TCP    66 8080 > 36650 [ACK] Seq=1 Ack=17 Win=2840 Len=0 TSval=1641592439 TSecr=3239584
10 2013-03-31 10:07:41.:120.204.201.154  192.168.137.87    TCP    84 [TCP segment of a reassembled PDU]
11 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   TCP    66 36650 > 8080 [ACK] Seq=17 Ack=19 Win=5856 Len=0 TSval=3239604 TSecr=1641592440
12 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   HTTP   692 Continuation or non-HTTP traffic
13 2013-03-31 10:07:41.:120.204.201.154  192.168.137.87    TCP    66 8080 > 36650 [ACK] Seq=19 Ack=643 Win=2856 Len=0 TSval=1641592486 TSecr=3239608
14 2013-03-31 10:07:41.:120.204.201.154  192.168.137.87    HTTP   1066 Continuation or non-HTTP traffic
15 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   TCP    66 36650 > 8080 [ACK] Seq=643 Ack=1019 Win=7840 Len=0 TSval=3239629 TSecr=1641592506
16 2013-03-31 10:07:41.:192.168.137.87   120.204.201.154   HTTP   297 Continuation or non-HTTP traffic
17 2013-03-31 10:07:41.:120.204.201.154  192.168.137.87    TCP    66 8080 > 36650 [ACK] Seq=1019 Ack=874 Win=2856 Len=0 TSval=1641592553 TSecr=3239635
18 2013-03-31 10:07:42.:120.204.201.154  192.168.137.87    HTTP   314 Continuation or non-HTTP traffic
19 2013-03-31 10:07:42.:192.168.137.87   120.204.201.154   TCP    66 36650 > 8080 [ACK] Seq=874 Ack=1267 Win=9856 Len=0 TSval=3239650 TSecr=1641592568
20 2013-03-31 10:07:42.:125.39.223.218   192.168.137.87    TCP    54 80 > 54318 [FIN, ACK] Seq=1 Ack=1 Win=54 Len=0
21 2013-03-31 10:07:42.:192.168.137.87   125.39.223.218    TCP    54 54318 > 80 [ACK] Seq=1 Ack=2 Win=283 Len=0
```

第 8 到第 19 包数据是客户端和服务器之前用 HTTP 协议相互传送了一些数据。

第 18 包是 HTTP 数据包，它的大小为 314 字节，其中有用数据长度为 248 字节，数据最后一行为空行，表明数据已经传送完毕，如下图所示：

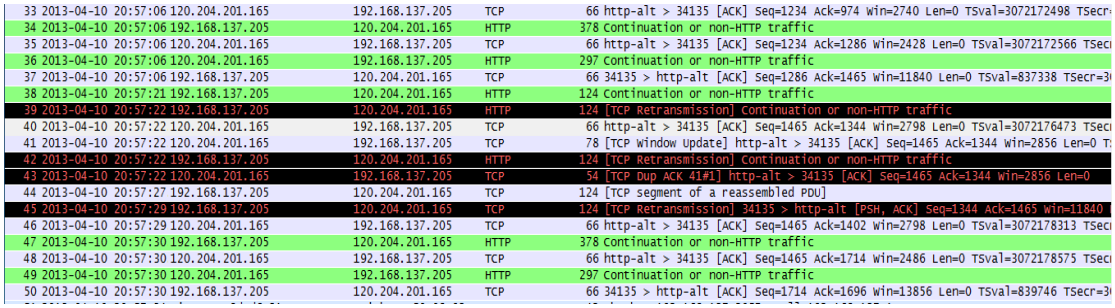
```
⊞ Frame 18: 314 bytes on wire (2512 bits), 314 bytes captured (2512 bits) on interface 0
⊞ Ethernet II, Src: LiteonTe_8d:d6:31 (70:f1:a1:8d:d6:31), Dst: TwinhanT_50:08:93 (00:08:ca:50:08:93)
⊞ Internet Protocol Version 4, Src: 120.204.201.154 (120.204.201.154), Dst: 192.168.137.87 (192.168.137.87)
⊞ Transmission Control Protocol, Src Port: 8080 (8080), Dst Port: 36650 (36650), Seq: 1019, Ack: 874, Len: 248
⊟ Hypertext Transfer Protocol
  ⊟ Data (248 bytes)
      Data: 000000f8001000013b9aca7900000016be810121feda0000...
      [Length: 248]
```

```
0000  00 08 ca 50 08 93 70 f1  a1 8d d6 31 08 00 45 00   ...P..p. ...1..E.
0010  01 2c 82 e5 00 00 31 06  79 80 78 cc c9 9a c0 a8   .,....1. y.x.....
0020  89 57 1f 90 8f 2a fb 2d  13 30 51 6b 27 22 80 18   .W...*.- .0Qk'"..
0030  05 94 42 9e 00 00 01 01  08 0a 61 d8 b6 f8 00 31   ..B..... ..a....1
0040  6e d3 00 00 00 f8 00 10  00 01 3b 9a ca 79 00 00   n....... ..;..y..
0050  00 16 be 81 01 21 fe da  00 00 00 00 00 00 00 01   .....!.. ........
0060  01 be 02 04 a5 77 7b 81  03 02 00 00 04 04 06 00   .....w{. ........
0070  00 00 05 06 00 00 00 00  00 00 06 10 41 35 30 62   ........ ....A50b
0080  36 64 33 61 32 37 31 33  33 39 63 00 07 02 e9 03   6d3a2713 39c.....
0090  08 02 01 00 09 02 05 00  0a 04 82 00 00 00 0b 04   ........ ........
00a0  77 00 00 00 0c 80 01 4d  95 46 7d b2 ae ea b3 8c   w......M .F}.....
00b0  a3 0f 1b 00 18 d7 54 45  cc be 0f 2a 54 f0 88 b9   ......TE ...*T...
00c0  a7 37 bb 57 9d e9 dd 67  0b d7 be bb 28 20 83 67   .7.W...g ....( .g
00d0  2e 40 96 9f d9 2d 06 7d  34 df 50 d3 19 66 ce a2   .@...-.} 4.P..f..
00e0  2c 21 da fd d1 9b 98 c7  64 5c 42 85 b5 56 05 28   ,!...... d\B..V.(
00f0  c4 b4 40 e4 21 5a 0d b0  07 6d 51 e5 56 78 84 3d   ..@.!Z.. .mQ.Vx.=
0100  fe 4e 42 a6 3b 97 ee f1  79 1b 1e 9a 67 ba 03 70   .NB.;... y...g..p
0110  85 95 c5 ef b0 84 97 66  4a ad ef 22 a1 34 99 3f   .......f J.."4.?
0120  72 d8 70 8c 29 cc 57 0d  04 00 00 00 00 0e 01 ed   r.p.).W. ........
0130  0f 04 00 00 00 00 10 01  ed ed                     ........ ..
```

第 20 和 21 包数据是关闭连接。传送完数据后，主机发出带 FIN 的 TCP 报文，要求关闭连接，客户端发出确认（第 21 包数据），连接关闭。

```
19 2013-03-31 10:07:42.:192.168.137.87   120.204.201.154   TCP    66 36650 > 8080 [ACK] Seq=874 Ack=1267 Win=9856 Len=0 TSval=3239650 T
20 2013-03-31 10:07:42.:125.39.223.218   192.168.137.87    TCP    54 80 > 54318 [FIN, ACK] Seq=1 Ack=1 Win=54 Len=0
21 2013-03-31 10:07:42.:192.168.137.87   125.39.223.218    TCP    54 54318 > 80 [ACK] Seq=1 Ack=2 Win=283 Len=0
```

超时会重传：

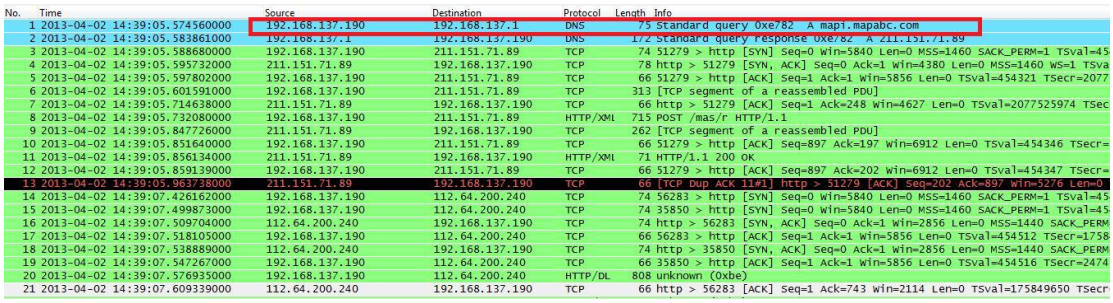


33	2013-04-10 20:57:06	120.204.201.165	192.168.137.205	TCP	66 http-alt > 34135 [ACK] Seq=1234 Ack=974 Win=2740 Len=0 TSval=3072172498 TSecr
34	2013-04-10 20:57:06	192.168.137.205	120.204.201.165	HTTP	378 Continuation or non-HTTP traffic
35	2013-04-10 20:57:06	120.204.201.165	192.168.137.205	TCP	66 http-alt > 34135 [ACK] Seq=1234 Ack=1286 Win=2428 Len=0 TSval=3072172566 TSecr
36	2013-04-10 20:57:06	120.204.201.165	192.168.137.205	HTTP	297 Continuation or non-HTTP traffic
37	2013-04-10 20:57:06	192.168.137.205	120.204.201.165	TCP	66 34135 > http-alt [ACK] Seq=1286 Ack=1465 Win=11840 Len=0 TSval=837338 TSecr=3
38	2013-04-10 20:57:21	192.168.137.205	120.204.201.165	HTTP	124 Continuation or non-HTTP traffic
39	2013-04-10 20:57:22	192.168.137.205	120.204.201.165	HTTP	124 [TCP Retransmission] Continuation or non-HTTP traffic
40	2013-04-10 20:57:22	120.204.201.165	192.168.137.205	TCP	66 http-alt > 34135 [ACK] Seq=1465 Ack=1344 Win=2798 Len=0 TSval=3072176473 TSecr
41	2013-04-10 20:57:22	120.204.201.165	192.168.137.205	TCP	78 [TCP Window Update] http-alt > 34135 [ACK] Seq=1465 Ack=1344 Win=2856 Len=0 T
42	2013-04-10 20:57:22	192.168.137.205	120.204.201.165	HTTP	124 [TCP Retransmission] Continuation or non-HTTP traffic
43	2013-04-10 20:57:22	120.204.201.165	192.168.137.205	TCP	54 [TCP Dup ACK 41#1] http-alt > 34135 [ACK] Seq=1465 Ack=1344 Win=2856 Len=0
44	2013-04-10 20:57:27	192.168.137.205	120.204.201.165	TCP	124 [TCP segment of a reassembled PDU]
45	2013-04-10 20:57:29	192.168.137.205	120.204.201.165	TCP	124 [TCP Retransmission] 34135 > http-alt [PSH, ACK] Seq=1344 Ack=1465 Win=11840
46	2013-04-10 20:57:29	120.204.201.165	192.168.137.205	TCP	66 http-alt > 34135 [ACK] Seq=1465 Ack=1402 Win=2798 Len=0 TSval=3072178313 TSecr
47	2013-04-10 20:57:30	192.168.137.205	120.204.201.165	HTTP	378 Continuation or non-HTTP traffic
48	2013-04-10 20:57:30	120.204.201.165	192.168.137.205	TCP	66 http-alt > 34135 [ACK] Seq=1465 Ack=1714 Win=2486 Len=0 TSval=3072178575 TSecr
49	2013-04-10 20:57:30	120.204.201.165	192.168.137.205	HTTP	297 Continuation or non-HTTP traffic
50	2013-04-10 20:57:30	192.168.137.205	120.204.201.165	TCP	66 34135 > http-alt [ACK] Seq=1714 Ack=1696 Win=13856 Len=0 TSval=839746 TSecr=3

第 39 包：未收到第 38 包数据的确认应答，超时后，开始重传；
第 42 包：第 38 包数据仍未收到应答，又超时，重传一次；
第 43 包：终于收到了第 38 包数据的应答。

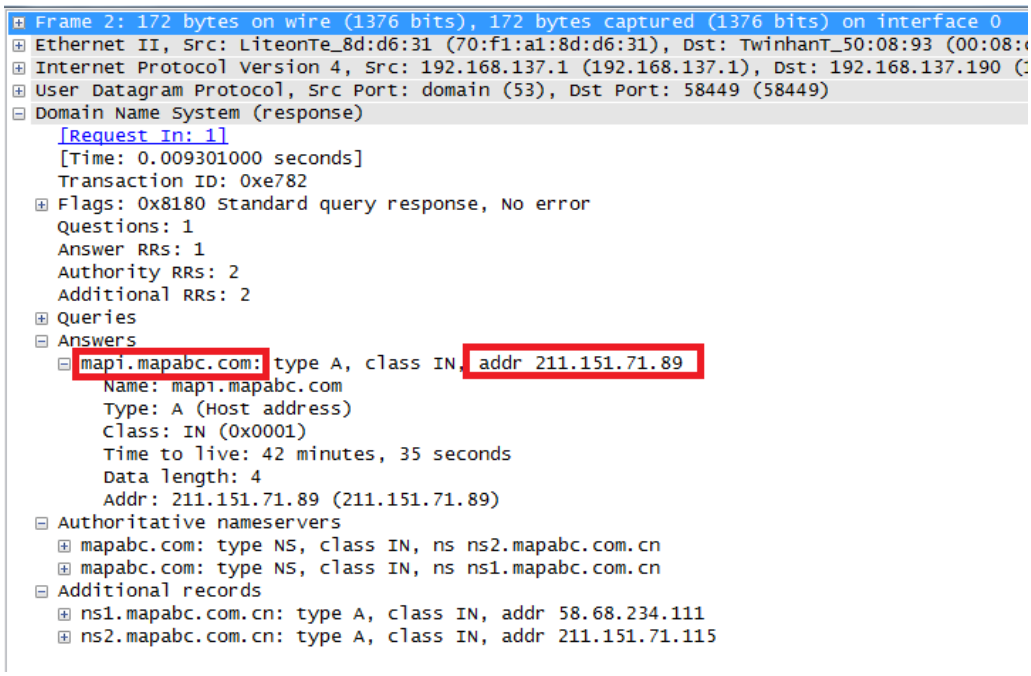
步骤 4. 微信-附近的人

用 wireshark 抓包得到如下数据



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-04-02 14:39:05.574560000	192.168.137.190	192.168.137.1	DNS	75	Standard query 0xe782 A mapi.mapabc.com
2	2013-04-02 14:39:05.583861000	192.168.137.1	192.168.137.190	DNS	172	Standard query response 0xe782 A 211.151.71.89
3	2013-04-02 14:39:05.588680000	192.168.137.190	211.151.71.89	TCP	74	51279 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=45
4	2013-04-02 14:39:05.595732000	211.151.71.89	192.168.137.190	TCP	78	http > 51279 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1460 WS=1 TSva
5	2013-04-02 14:39:05.597802000	192.168.137.190	211.151.71.89	TCP	66	51279 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=454321 TSecr=2077
6	2013-04-02 14:39:05.601591000	192.168.137.190	211.151.71.89	TCP	313	[TCP segment of a reassembled PDU]
7	2013-04-02 14:39:05.714638000	211.151.71.89	192.168.137.190	TCP	66	http > 51279 [ACK] Seq=1 Ack=248 Win=4627 Len=0 TSval=2077525974 TSec
8	2013-04-02 14:39:05.732080000	192.168.137.190	211.151.71.89	HTTP/XML	715	POST /mas/r HTTP/1.1
9	2013-04-02 14:39:05.847726000	211.151.71.89	192.168.137.190	TCP	262	[TCP segment of a reassembled PDU]
10	2013-04-02 14:39:05.851640000	192.168.137.190	211.151.71.89	TCP	66	51279 > http [ACK] Seq=897 Ack=197 Win=6912 Len=0 TSval=454346 TSecr=
11	2013-04-02 14:39:05.856134000	211.151.71.89	192.168.137.190	HTTP/XML	71	HTTP/1.1 200 OK
12	2013-04-02 14:39:05.859139000	192.168.137.190	211.151.71.89	TCP	66	51279 > http [ACK] Seq=897 Ack=202 Win=6912 Len=0 TSval=454347 TSecr=
13	2013-04-02 14:39:05.963738000	211.151.71.89	192.168.137.190	TCP	66	[TCP Dup ACK 11#1] http > 51279 [ACK] Seq=202 Ack=897 Win=5276 Len=0
14	2013-04-02 14:39:07.426162000	192.168.137.190	112.64.200.240	TCP	74	56283 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=45
15	2013-04-02 14:39:07.499873000	192.168.137.190	112.64.200.240	TCP	74	35850 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=45
16	2013-04-02 14:39:07.509704000	112.64.200.240	192.168.137.190	TCP	74	http > 56283 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM
17	2013-04-02 14:39:07.518105000	192.168.137.190	112.64.200.240	TCP	66	56283 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=454512 TSecr=1758
18	2013-04-02 14:39:07.538889000	112.64.200.240	192.168.137.190	TCP	74	http > 35850 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM
19	2013-04-02 14:39:07.547267000	192.168.137.190	112.64.200.240	TCP	66	35850 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=454516 TSecr=2474
20	2013-04-02 14:39:07.576935000	192.168.137.190	112.64.200.240	HTTP/DL	808	unknown (0xbe)
21	2013-04-02 14:39:07.609339000	112.64.200.240	192.168.137.190	TCP	66	http > 56283 [ACK] Seq=1 Ack=743 Win=2114 Len=0 TSval=175849650 TSecr

首先是 DNS 解析，展开第二包数据，可以看到



```
⊞ Frame 2: 172 bytes on wire (1376 bits), 172 bytes captured (1376 bits) on interface 0
⊞ Ethernet II, Src: LiteonTe_8d:d6:31 (70:f1:a1:8d:d6:31), Dst: TwinhanT_50:08:93 (00:08:
⊞ Internet Protocol Version 4, Src: 192.168.137.1 (192.168.137.1), Dst: 192.168.137.190 (
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: 58449 (58449)
⊟ Domain Name System (response)
    [Request In: 1]
    [Time: 0.009301000 seconds]
    Transaction ID: 0xe782
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ⊞ Queries
  ⊟ Answers
    ⊟ mapi.mapabc.com: type A, class IN, addr 211.151.71.89
        Name: mapi.mapabc.com
        Type: A (Host address)
        Class: IN (0x0001)
        Time to live: 42 minutes, 35 seconds
        Data length: 4
        Addr: 211.151.71.89 (211.151.71.89)
  ⊟ Authoritative nameservers
    ⊞ mapabc.com: type NS, class IN, ns ns2.mapabc.com.cn
    ⊞ mapabc.com: type NS, class IN, ns ns1.mapabc.com.cn
  ⊟ Additional records
    ⊞ ns1.mapabc.com.cn: type A, class IN, addr 58.68.234.111
    ⊞ ns2.mapabc.com.cn: type A, class IN, addr 211.151.71.115
```

DNS 应答返回了域名 mapi.mapabc.com 的 IP：211.151.71.89

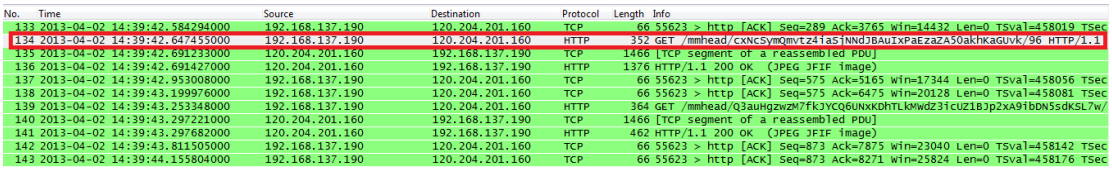
mapabc.com 是北京图盟科技有限公司的网站，是一家致力于互联网地图、手机地图和相关位置服务的互联网软件技术服务公司，它是高德成员企业。（有个高德地图的 app）

随后的几包数据，是客户端和该服务器之间相互交换信息。

查询该 IP.发现服务器位于北京。

可以看到，微信客户端的地点信息被收集起来存储在服务器中，当客户端发送附近的人请求时，服务器调用地图信息，通过计算，得到位于附近的用户数据，将它们传给该客户端。

附近的人---用户头像下载过程



No.	Time	Source	Destination	Protocol	Length	Info
133	2013-04-02 14:39:42.584294000	192.168.137.190	120.204.201.160	TCP	66	55623 > http [ACK] Seq=289 Ack=3765 Win=14432 Len=0 TSval=458019 TSec
134	2013-04-02 14:39:42.647455000	192.168.137.190	120.204.201.160	HTTP	352	GET /mmhead/cxNcSymQmvtz4iaSjNNdJBAuIxPaEzaZA50akhKaGUvk/96 HTTP/1.1
135	2013-04-02 14:39:42.691233000	120.204.201.160	192.168.137.190	TCP	1466	[TCP segment of a reassembled PDU]
136	2013-04-02 14:39:42.691427000	120.204.201.160	192.168.137.190	HTTP	1376	HTTP/1.1 200 OK (JPEG JFIF image)
137	2013-04-02 14:39:42.953008000	192.168.137.190	120.204.201.160	TCP	66	55623 > http [ACK] Seq=575 Ack=5165 Win=17344 Len=0 TSval=458056 TSec
138	2013-04-02 14:39:43.199976000	192.168.137.190	120.204.201.160	TCP	66	55623 > http [ACK] Seq=575 Ack=6475 Win=20128 Len=0 TSval=458081 TSec
139	2013-04-02 14:39:43.253348000	192.168.137.190	120.204.201.160	HTTP	364	GET /mmhead/Q3auHgzwzM7fkJYCQ6UNxKDhTLkMWdZ3icUZ1BJp2xA9ibDN55dKSL7w/
140	2013-04-02 14:39:43.297221000	120.204.201.160	192.168.137.190	TCP	1466	[TCP segment of a reassembled PDU]
141	2013-04-02 14:39:43.297682000	120.204.201.160	192.168.137.190	HTTP	462	HTTP/1.1 200 OK (JPEG JFIF image)
142	2013-04-02 14:39:43.811505000	192.168.137.190	120.204.201.160	TCP	66	55623 > http [ACK] Seq=873 Ack=7875 Win=23040 Len=0 TSval=458142 TSec
143	2013-04-02 14:39:44.155804000	192.168.137.190	120.204.201.160	TCP	66	55623 > http [ACK] Seq=873 Ack=8271 Win=25824 Len=0 TSval=458176 TSec

第 134 包： HTTP 的 GET 请求，展开该包：

```
⊞ Frame 134: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits) on interface 0
⊞ Ethernet II, Src: TwinhanT_50:08:93 (00:08:ca:50:08:93), Dst: LiteonTe_8d:d6:31 (70:f1:a1:8d:d6:31)
⊞ Internet Protocol Version 4, Src: 192.168.137.190 (192.168.137.190), Dst: 120.204.201.160 (120.204.201.160)
⊞ Transmission Control Protocol, Src Port: 55623 (55623), Dst Port: http (80), Seq: 289, Ack: 3765, Len: 286
⊟ Hypertext Transfer Protocol
  ⊟ GET /mmhead/cxNcSymQmvtz4iaSjNNdJBAuIxPaEzaZA50akhKaGUvk/96 HTTP/1.1\r\n
    ⊟ [Expert Info (Chat/Sequence): GET /mmhead/cxNcSymQmvtz4iaSjNNdJBAuIxPaEzaZA50akhKaGUvk/96 HTTP/1.1\r\n]
        [Message: GET /mmhead/cxNcSymQmvtz4iaSjNNdJBAuIxPaEzaZA50akhKaGUvk/96 HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /mmhead/cxNcSymQmvtz4iaSjNNdJBAuIxPaEzaZA50akhKaGUvk/96
      Request Version: HTTP/1.1
  referer: http://weixin.qq.com/?version=604307714&uin=2172352421\r\n
  User-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.4; Lenovo S760 Build/GINGERBREAD)\r\n
  Host: wx.qlogo.cn\r\n
  Connection: Keep-Alive\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http://wx.qlogo.cn/mmhead/cxNcSymQmvtz4iaSjNNdJBAuIxPaEzaZA50akhKaGUvk/96]
```

将请求的地址输入到浏览器，会看到一个用户头像；

第 135 包 是服务器端的 TCP 协议将该头像分段成两段(第 135 包和 136 包)，传送给客户端；

第 136 包 标为 HTTP 包，表示头像传送出去了。

第 137 和 138 包 客户端收到 HTTP 传来的头像后，向服务器发 TCP 确认，传送完成。

三. 实验结论:关于微信协议

1.微信通过内置浏览器和服务器交互数据。

微信在应用层使用 HTTP 协议传输数据。微信的聊天对话框如下，点击网址链接，会跳转到浏览器模式，打开该消息对应的网页。现在手机 QQ 和微博客户端都内置了浏览器。而且用 wireshark 抓包发现微信的通信都是用 HTTP 协议收发数据的，内嵌浏览器为网络通信接口。

2.微信的数据传输未加密

微信只有在输入密码的**初次认证**过程中的数据是用 SSL 加密传输的。其他数据，比如聊天数据，地理位置信息等，传输过程都没有加密（源端加密未知）

192.168.137.175	192.168.137.1	DNS	78 Standard query 0xc368 A long.weixin.qq.com
192.168.137.1	192.168.137.175	DNS	346 Standard query response 0xc368 A 120.204.201.151 A 120.204.201.154 A 1
192.168.137.175	long.weixin.qq.com	TCP	74 49741 > https [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=655
long.weixin.qq.com	192.168.137.175	TCP	74 https > 49741 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM=
192.168.137.175	long.weixin.qq.com	TCP	66 49741 > https [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=6559616 TSecr=6391
192.168.137.175	long.weixin.qq.com	SSL	82 Continuation Data
long.weixin.qq.com	192.168.137.175	TCP	66 https > 49741 [ACK] Seq=1 Ack=17 Win=2840 Len=0 TSval=639155318 TSecr=6
long.weixin.qq.com	192.168.137.175	SSL	84 Continuation Data
192.168.137.175	long.weixin.qq.com	TCP	66 49741 > https [ACK] Seq=17 Ack=19 Win=5856 Len=0 TSval=6559627 TSecr=63
192.168.137.175	long.weixin.qq.com	SSL	692 Continuation Data
long.weixin.qq.com	192.168.137.175	TCP	66 https > 49741 [ACK] Seq=19 Ack=643 Win=2856 Len=0 TSval=639155363 TSecr
long.weixin.qq.com	192.168.137.175	SSL	1130 Continuation Data
192.168.137.175	long.weixin.qq.com	TCP	66 49741 > https [ACK] Seq=643 Ack=1083 Win=7968 Len=0 TSval=6559658 TSecr
192.168.137.1	192.168.137.175	ARP	42 Who has 192.168.137.175? Tell 192.168.137.1
192.168.137.175	192.168.137.1	ARP	42 192.168.137.175 is at 00:08:ca:50:08:93

总结：微信各个功能的数据传输，几乎全都是用 HTTP 协议

3.微信不同功能有独立的服务器：

①涉及到位置信息，会调用地图，常用的有：

map.soso.com　　搜搜地图

maps.google.com　　谷歌地图

mapi.mapabc.com　　高德地图

```
ff02::1:3                LLMNR      84 Standard query 0x30ca  A wpad
224.0.0.252              LLMNR      64 Standard query 0x30ca  A wpad
ff02::1:3                LLMNR      84 Standard query 0x30ca  A wpad
224.0.0.252              LLMNR      64 Standard query 0x30ca  A wpad
192.168.137.1            DNS        79 Standard query 0x820a  A apikey.map.soso.com
192.168.137.105          DNS       208 Standard query response 0x820a  CNAME rtt.map.soso.com A 58.251.149.11
192.168.137.1            DNS        75 Standard query 0x01ab  A maps.google.com
192.168.137.105          DNS       433 Standard query response 0x01ab  CNAME maps.l.google.com CNAME maps-chi
192.168.137.1            DNS        74 Standard query 0x5ffd  A p.map.soso.com
192.168.137.105          DNS       153 Standard query response 0x5ffd  A 59.74.42.67 A 59.74.42.68
ff02::1:3                LLMNR      84 Standard query 0x4f94  A wpad
224.0.0.252              LLMNR      64 Standard query 0x4f94  A wpad
ff02::1:3                LLMNR      84 Standard query 0x4f94  A wpad
224.0.0.252              LLMNR      64 Standard query 0x4f94  A wpad
ff02::1:3                LLMNR      84 Standard query 0x9e45  A wpad
```

②微信的好多图片文件的访问，都是对 **wx.qlogo.cn** 和 **mmsns.qpic.cn** 的

```
23 2013-03-29 20:26:23.(192.168.137.186  wx.qlogo.cn          HTTP    277 GET /mmhead/nIxiad2zLwx3q0gjdXWOtH6cVmYZKgZViaAibuGqQaTU94/96 HTTP/1.1
24 2013-03-29 20:26:23. wx.qlogo.cn      192.168.137.186     TCP      54 http > 40460 [ACK] Seq=3130 Ack=447 Win=7504 Len=0
25 2013-03-29 20:26:23. wx.qlogo.cn      192.168.137.186     TCP    1466 [TCP segment of a reassembled PDU]
26 2013-03-29 20:26:23.(192.168.137.186  wx.qlogo.cn          TCP      54 40460 > http [ACK] Seq=447 Ack=4542 Win=16944 Len=0
27 2013-03-29 20:26:23. wx.qlogo.cn      192.168.137.186     TCP    1466 [TCP segment of a reassembled PDU]
28 2013-03-29 20:26:23.(192.168.137.186  wx.qlogo.cn          TCP      54 40460 > http [ACK] Seq=447 Ack=5954 Win=19768 Len=0
29 2013-03-29 20:26:23. wx.qlogo.cn      192.168.137.186     HTTP    359 HTTP/1.1 200 OK  (JPEG JFIF image)
30 2013-03-29 20:26:23.(192.168.137.186  wx.qlogo.cn          TCP      54 40460 > http [ACK] Seq=447 Ack=6259 Win=22592 Len=0
31 2013-03-29 20:26:24.(192.168.137.186  192.168.137.1        DNS      73 Standard query 0x4df1  A mmsns.qpic.cn
32 2013-03-29 20:26:24.(192.168.137.1    192.168.137.186      DNS     139 Standard query response 0x4df1  A 112.65.195.147
33 2013-03-29 20:26:25.(192.168.137.186  mmsns.qpic.cn        TCP      74 34946 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=408568 TSecr=0 WS=32
34 2013-03-29 20:26:26.(192.168.137.1    192.168.137.186      ARP      42 Who has 192.168.137.186?  Tell 192.168.137.1
35 2013-03-29 20:26:26.(192.168.137.186  192.168.137.1        ARP      42 192.168.137.186 is at 00:08:ca:50:08:93
36 2013-03-29 20:26:28.(192.168.137.186  mmsns.qpic.cn        TCP      74 34946 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=408869 TSecr=0 WS=32
37 2013-03-29 20:26:28. mmsns.qpic.cn    192.168.137.186     TCP      74 http > 34946 [SYN, ACK] Seq=0 Ack=1 Win=5600 Len=0 MSS=1412 SACK_PERM=1 TSval=331001535 TS
38 2013-03-29 20:26:28.(192.168.137.186  mmsns.qpic.cn        TCP      66 34946 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=408876 TSecr=331001535
39 2013-03-29 20:26:28.(192.168.137.186  mmsns.qpic.cn        HTTP    299 GET /mmsns/mx1G2uouIqkPpqk1zlGPvLFSCFbCmLmt6YTmfhVrpJvzjTvZZ9kZRQ/150 HTTP/1.1
```

③微信登陆的时候，有两个域名：**long.weixin.qq.com** 和 **short.weixin.qq.com**

```
15 2013-04-02 17:22:00.(192.168.137.212  192.168.137.1        DNS      78 Standard query 0xd2ef  A long.weixin.qq.com
16 2013-04-02 17:22:00.(192.168.137.1    192.168.137.212      DNS     346 Standard query response 0xd2ef  A 117.135.130.187 A 120.204.201.151 A 120.204.201.154 A 12
17 2013-04-02 17:22:00.(192.168.137.212  long.weixin.qq.com    TCP      74 40772 > http-alt [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=382690 TSecr=0 WS=3
18 2013-04-02 17:22:02.(fe80::795e:cf0a:b12ff02::1:2         DHCPv6   148 Solicit XID: 0x7068d0 CID: 0001000118257f37c80aa9b8dfcc
19 2013-04-02 17:22:03.(192.168.137.212  long.weixin.qq.com    TCP      74 40772 > http-alt [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=382999 TSecr=0 WS=3
20 2013-04-02 17:22:03.(long.weixin.qq.com 192.168.137.212    TCP      74 http-alt > 40772 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM=1 TSval=32339485
21 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    TCP      66 40772 > http-alt [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=383059 TSecr=32339485
22 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    TCP      82 [TCP segment of a reassembled PDU]
23 2013-04-02 17:22:04.(long.weixin.qq.com 192.168.137.212    TCP      66 http-alt > 40772 [ACK] Seq=1 Ack=17 Win=2840 Len=0 TSval=32339566 TSecr=383060
24 2013-04-02 17:22:04.(long.weixin.qq.com 192.168.137.212    TCP      84 [TCP segment of a reassembled PDU]
25 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    TCP      66 40772 > http-alt [ACK] Seq=17 Ack=19 Win=5856 Len=0 TSval=383065 TSecr=32339566
26 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    HTTP    692 Continuation or non-HTTP traffic
27 2013-04-02 17:22:04.(long.weixin.qq.com 192.168.137.212    TCP      66 http-alt > 40772 [ACK] Seq=19 Ack=643 Win=2856 Len=0 TSval=32339597 TSecr=383069
28 2013-04-02 17:22:04.(long.weixin.qq.com 192.168.137.212    HTTP    922 Continuation or non-HTTP traffic
29 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    TCP      66 40772 > http-alt [ACK] Seq=643 Ack=875 Win=7552 Len=0 TSval=383087 TSecr=32339621

30 2013-04-02 17:22:04.(192.168.137.212  192.168.137.1        DNS      79 Standard query 0xeaf8  A short.weixin.qq.com
31 2013-04-02 17:22:04.(192.168.137.1    192.168.137.212      DNS     171 Standard query response 0xeaf8  A 112.64.200.240 A 112.64.237.186
32 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    HTTP    281 Continuation or non-HTTP traffic
33 2013-04-02 17:22:04.(long.weixin.qq.com 192.168.137.212    TCP      66 http-alt > 40772 [ACK] Seq=875 Ack=858 Win=2856 Len=0 TSval=32339660 TSecr=383096
34 2013-04-02 17:22:04.(192.168.137.212  short.weixin.qq.com   TCP      74 52819 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=383103 TSecr=0 WS=32
35 2013-04-02 17:22:04.(long.weixin.qq.com 192.168.137.212    HTTP    281 Continuation or non-HTTP traffic
36 2013-04-02 17:22:04.(short.weixin.qq.com192.168.137.212    TCP      74 http > 52819 [SYN, ACK] Seq=0 Ack=1 Win=2856 Len=0 MSS=1440 SACK_PERM=1 TSval=2477200195 T
37 2013-04-02 17:22:04.(192.168.137.212  short.weixin.qq.com   TCP      66 52819 > http [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=383128 TSecr=2477200195
38 2013-04-02 17:22:04.(192.168.137.212  long.weixin.qq.com    TCP      66 40772 > http-alt [ACK] Seq=858 Ack=1090 Win=9280 Len=0 TSval=383128 TSecr=32339672
39 2013-04-02 17:22:04.(192.168.137.212  short.weixin.qq.com HTTP/DL   505 unknown (0xbe)
40 2013-04-02 17:22:04.(LiteonTe_8d:d6:31  Twinhant_50:08:93   ARP      42 Who has 192.168.137.212?  Tell 192.168.137.1
41 2013-04-02 17:22:04.(Twinhant_50:08:93  LiteonTe_8d:d6:31   ARP      42 192.168.137.212 is at 00:08:ca:50:08:93
42 2013-04-02 17:22:04.(short.weixin.qq.com192.168.137.212    TCP      66 http > 52819 [ACK] Seq=1 Ack=440 Win=2416 Len=0 TSval=2477200263 TSecr=383130
43 2013-04-02 17:22:04.(short.weixin.qq.com192.168.137.212    HTTP/DL  505 unknown (0xbe)
44 2013-04-02 17:22:04.(192.168.137.212  short.weixin.qq.com   TCP      66 52819 > http [ACK] Seq=440 Ack=440 Win=6912 Len=0 TSval=383138 TSecr=2477200268
45 2013-04-02 17:22:04.(192.168.137.212  short.weixin.qq.com   TCP      66 52819 > http [FIN, ACK] Seq=440 Ack=440 Win=6912 Len=0 TSval=383141 TSecr=2477200268
46 2013-04-02 17:22:04.(short.weixin.qq.com192.168.137.212    TCP      66 http > 52819 [FIN, ACK] Seq=440 Ack=441 Win=2856 Len=0 TSval=2477200289 TSecr=383141
47 2013-04-02 17:22:05.(192.168.137.212  short.weixin.qq.com   TCP      66 52819 > http [ACK] Seq=441 Ack=441 Win=6912 Len=0 TSval=383152 TSecr=2477200289
48 2013-04-02 17:22:05.(192.168.137.212  short.weixin.qq.com   TCP      74 52689 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=383212 TSecr=0 WS=32
```

short.weixin.qq.com　是 HTTP 协议扩展

tcp 短连接，运行 8080 port，http body 为二进制。

提供 API：

用户登录验证;

好友关系（获取，添加）；
消息 sync (newsync)，自有 sync 机制；
获取用户图像；
用户注销；
行为日志上报。

long.weixin.qq.com
tcp 长连接， 端口为 8080，类似微软 activesync 的二进制协议。
提供 API：
接受/发送文本消息；
接受/发送语音；
接受/发送图片；
接受/发送视频文件等。

4.关于"微信与运营商大战"的思考：

TCP 短连接是指通讯双方有数据交互时，建立一个连接，数据发送完成后，则断开此连接，即每次连接只完成一项业务的发送；TCP 长连接，是指连接建立后保持较长时间而不释放掉。Android 默认的推送服务，采用的是 Google 的 GCM 技术，其心跳周期约为 28 分钟，这才是所谓“慢”的含义 —— 尽可能降低心跳的频度，从而达到省电、省流量的目的。

微信客户端与服务器之间的大部分连接都是 TCP 长连接，慢心跳。本来是为了能够给用户提供即使提醒和通知的方便并为用户节约耗电。但在中国大陆的 2.5G 网络中，如果闲置超过大概 5 分钟，运营商的 IP 网关会自动释放掉（关闭）连接，心跳周期远远达不到 28 分钟。为此，Android 版本的微信选择以 5 分钟为周期发送心跳连接。这种过于频繁的心跳连接，加上微信庞大的用户数量，导致了网络信令的严重占用。这是最近微信和网络运营商之间矛盾的原因之一。而且，每一次心跳，都相当于把手机从待机状态唤醒，以 5 分钟为一个周期，每天最大约 300 次唤醒，这会严重消耗手机的电量。

因此，从共赢的角度讲，运营商方面，应该升级网络，加速网络建设，合理收费；而腾讯公司应该优化微信软件，尽量减少网络占用，以期能达到一个平衡。其实微信带来的问题远不止信令占用这一项，更重要的是，微信的通信模式，使传统的话音业务和短信业务受到巨大冲击，尤其微信对短信业务的侵蚀非常大，这才是触及运营商利益的最大头 。其实这也是一个无法避免的发展趋势，通信业的发展重心，已经开始由话音业务转向网络业务，随着 3G 和 4G 网络的建设，相信微信所引起的矛盾最终会得到解决。

参考文献：

【1】微信分析 http://blog.sina.com.cn/s/blog_5f92b32f0101bi3w.html
【2】微信的研究 http://blog.csdn.net/chief1985/article/details/7902016
【3】微信的研究（二）http://blog.csdn.net/chief1985/article/details/7905540
【4】微信架构（转）http://www.cnblogs.com/SuperXJ/archive/2012/05/29/2523411.html
【5】微信收费事件背后被广泛忽略的技术细节
http://tech.sina.com.cn/i/csj/2013-04-16/09368244003.shtml?bsh_bid=219839275
【6】TCP 协议的一些总结（一）
http://www.cnblogs.com/geekma/archive/2012/10/23/2735944.html
【7】TCP 几个字段含义 http://blog.sina.com.cn/s/blog_566c7d770101e7o7.html
【8】TCP 通信过程简介
http://hi.baidu.com/ncfjlwdvuwbgpud/item/4059b4ec69e865fbe0a5d485
【9】Wireshark 基本介绍和学习 TCP 三次握手
http://www.cnblogs.com/TankXiao/archive/2012/10/10/2711777.html#othertool
【10】Wireshark 实用过滤表达式
http://blog.163.com/szy8706@yeah/blog/static/6271318520123263141343 4/