**QQ通信协议介绍**

2009-09-18 17:29:11|  分类： [学习资料](http://etian4ever.blog.163.com/blog/#m=0&t=1&c=fks_087071093083083070082094094095086081082070081081080070)|字号 订阅

要通过抓取数据包来破争QQ密码.首先要对QQ的通信协议有一定的了解.只是通过抓包来分析的话,工作量是相当巨大的.幸好现在网上有一些开源的QQ项目.例如lumaqq.perl-oicq等.这要关我们就可以轻易了解QQ基本的通信协议了.QQ的通信协议是一套基于二进制数据的自己开发的应用层网络协议.其中使用一些公司的加密算法.QQ基本通信协议支持udp和tcp两种基本协议方式.两种方式的基本数据结构是一样的.只是tcp包多了一个描述长度的头部.那么我们就来看看QQ的登录过程是怎么样.  
首先QQ客户端向服务器发送一个请求登录令牌的数据包.服务器返回登录令牌.这个令牌是在服务器端生成的.和客户端的IP地址,版本信息等数据相关.以后会用到这个令牌去进行其他操作.  
在QQ客户端得到登录令牌之后.就会向服务器发送一个包含登录信息的登录请求.要求登录.服务顺会首先看看客户端的号码.I守址和版本是否可以在本服务器上进行登录.如果可以的话,就验证客户端的登录信息是否与服务器上保存的登录信息进行比较.匹配的就向客户端返回一个登录成功的数据包.不匹配返回登录失败.因为QQ的服务器有很多台.可能要分管不同的QQ版本.IP等.所以如果客户端的号码.IP地址和版本无法在本服务器进行登录.服务器就返蜀犬吠日一个重定向包.让客户端去另外一台服务器登录.其实整个QQ登录过程就是这么简单的两个步骤.  
了解了QQ登录的过程后.我们还需要知道具人本的数据包格式.以便解析出我们需要的数据内容.QQ登录过程的数据包分为头部.内容和尾部三个部分.其中头的格式固定为:0x02客户端版本 命令 序列号 QQ号码. 其中0x02是1个字节的标志;客户端版本2个字节.用于表示QQ客户端的版本;命令2个字节.表示要发送的命令类型.例如请求登录令牌登录请求等;序列号是一个2字节的随机数,在一次QQ会话中通过它来确认回应包是否对应请求包.QQ客户端默认每次加1;QQ号码就是4字节的QQ号.对于服务器来说是每个字段是无所谓的.QQ登录过程数据包的尾部固定为0x03.  
1. 请求登录令牌包  
包内容就是对一次命令的具体信息,对于第一次发送的请求登录令牌包来说,包命令是0x0062,整个请求包如下所示;   
而服务器返回包则相对复杂一些,如下所示;  
  
  
其中0x18表示登录令牌的长度,现在QQ默认的登录令牌长度是0x18.这个令牌是在服务器端生成的.具体的生成算法我们当然还无从得知,应该是参考了 QQ客户端的I守址.端口和其他一些信息生成这个令版的,因为你把在A机器上得到的令牌用到B机器上,你就会登录不了.如果你把A机器上的IP给改了.你照样也登录不了.  
2. 登录包.  
对于我们嗅探QQ密码来说,最重要的就是这个登录包.在这里包含了和QQ密码相关的信息.登录包的具体结构如下;  
  
   其中初始密钥是一个16字节的随机数,用于本身的加密.这里最重要的就是密码密钥加密的一个空字符串.  
   所谓密码密钥就是用QQ口呤进行两次MD5加密后得到的密文,然后以这个密文作为密钥去加密一个空字符串,这次加密使用了反馈的TEA算法,加密结果放在 QQ登录包里,让服务器去验证,由于QQ的加密算法使用特殊的填充机制使用QQ服务器可以验证出用户密码是否正确,这个会在后面进行详细的解释.QQ登录包里面还有一些诸如登录状态,登录令版和很多未知的内容.但是这些对于我们破解QQ密码来说都没有什么太大的作用.  
需要特别提到的是,前面的请求登录令牌包是不加密的,而这个登录包除了初始密钥本身以外的部分都要用初始密钥进行加密,加密算法同样是反馈的TEA.  
QQ服务器在收到这个登录包之后,首先要用初始密钥解密登录包后面的部分,如果解密成功,就会用保存在服务器上的密信息去解密密码密钥加密的那个空字符串密文,我现在还不确定QQ服务器上保存的是密码明文还是密码密钥.猜测是密码密钥.这样服务器就用密码密钥去解密那段16位密文,如果用户提交的密码是正确的.才可以解密成功.否则解密函数会返回空,认证就失败了.当验证QQ客户端密码准确无误后.就返回一个登录成功包.格式如下:  
  
QQ的加密算法  
了解了上面的QQ登录的通信协议之后还不足以破解QQ密码,我们还需要掌握QQ的加密算法.前面提到了,密码密钥是用户密码进行两次MD5加密之后得到的结果.然后再用空个结果作为密钥使用TEA算法进行加密.TEA是Tiny Encrypt Arithmetic的缩写.顾名思义就是一种比较简单的小型加密算法.它用一个16字节的密钥去加密一个8字节的明文.得到一个8字节的密文.也可以反向从密文解密出明文.具体的算法可以到网上搜索查阅.这里就不在赘述了.  
但是QQ使用的TEA虽然是标准的TEA.但是QQ却使用了一种自己特殊的填充反馈机制,QQ消息被分为多个加密单元.每一个加密单元都是8字节.使用 TEA进行加密.加密结果再作为下一个单元的密钥.如果明文本身的长度不是8的倍数.那么还要进行填充.使其成为8的倍数.填充的时候会用一个32位随机数存放于明文的开始位置.再在明文的最后用0填充为整个长度是8的倍数.由于会向后反馈这样即使对于相同的明文,因为使用了不同的随机数.也会产生完全不同的密文.  
使用这种特殊的填充反馈算法所导致的结果就是,一段密文只能用加密它的密钥进行解密.如果使用不正确的密钥.就无法得到正确的填充结果.最常见的就是解密后得到的填充数值不是0,这样就判断解密失败.  
服务器正式根据这种机制来确定客户端口的密码是否正确的.这也是我们破解QQ密的原理所在.  
穷举破解QQ密码  
有了以上的思路.只要写出程序就可以实现QQ密码的破解了.首先是抓包.我使用了winpcap来抓包.这样在HUB环境下可以抓到所有的QQ包.在交换环境中.我们可以使用一些ARP欺骗工具.同样可以抓到特定IP所发出的包.还有QQ的加密算法的实现.参考网上的perl-oicq和lumaqq等代码也可以轻易实现.然后用字典或者暴力破解的方法对密文进行解密即可.解密的过程用伪代码表示如下:结果=decrypt(密文,MD5(MD5(密码))),如果结果不为空的时候就是正确的密码.

[](http://www.lofter.com/)

[QQ协议研究1 -- 基于HTTP的QQ协议研究](http://yunfei3431.blog.163.com/blog/static/11524422520116248643936/)

[写给设计人的10个jQuery特效](http://yunfei3431.blog.163.com/blog/static/115244225201162484955392/)

**QQ通讯协议**

2011-07-24 20:18:58|  分类： [.NET](http://yunfei3431.blog.163.com/blog/#m=0&t=1&c=fks_084064086095083068085081094095085087084065080082084065081)|字号 订阅

要通过截取数据包来破解QQ密码，首先要对QQ的通信协议有一定了解。只是通过抓包来分析的话，工作量相当巨大的，幸好现在网上有一些开源的QQ项目，例如LumaQQ 、Perl-Oicq。这样我们就可以轻易了解到QQ基本的通信协议，

   QQ 的通信协议是一套基于二进制的数据自主开发的应用层网络协议，其中使用了一些公开的加密算法，QQ基本通信协议支持UDP和TCP两种基本协议方式。两种 方式的基本数据结构是一样的，只是TCP包多了一个描述长度的头部，那么我们就来看看QQ的登录过程是怎样的。

    首先QQ 客户端向服务器发送一个请求登录令牌的数据包，服务器返回登录令牌。这个令牌是在服务器端生成的，和客户端的IP地址，版本信息等数据相关。下文会用到这个令牌去进行其他操作。

   在QQ客户端得到登录令牌后，就会向服务器发送一个包含登录信息的登录请求，服务器首先会查看客户端的号码、IP地址和版本是否可以在本服务器上进行登 录，如果可以就验证客户端的登录信息是否与服务器上保存的登录信息一致，如果一致就向客户端返回一个连接成功的数据包，不匹配则返回登录失败，其实整个 QQ登录过程就是这么简单的两个步骤，如图1所示

   了解了QQ登录的过程后，我们还需要知道具体的数据包格式。以便解析出我们需要的数据内容，QQ登录过程的数据包分头部，内容和尾部三部分。其中头部的格式固定为：

 0x02 |  客户端版本 | 命令 | 序列号 | QQ号码

其中0x02是1个字节的标志，客户端版本2个字节，用于表示QQ客户端的版本，命令2字节，表示要发送的命令类型，例如请求登录令牌，登录请求 等；序列号是一个2字节的随机数，在一次QQ回话中通过它来确认回应包是否对应请求包，QQ客户端默认每次加1； QQ号码是4字节的QQ号，对于服务器来说这个字段是无所谓的。QQ登录过程数据包的尾部固定为0x03

**1。请求登录令牌包**

包内容就是一条命令的具体信息。对于第一次发送的请求登录令牌包来说，包命令是0x0062，整个请求包如下所示：

1. 头部

2. 0x00

3.尾部

而服务器返回包则相对复杂一些，如下所示：

1. 头部

2. 回复码 0x00表示成功，1字节

3. 登录令牌长度，默认为0x18

4. 登录令牌

5.尾部

其中0x18表示登录令牌的长度，现在QQ默认的登录令牌长度是0x018。此令牌是在服务器端生成的，具体的生成算法我们当然无从得知。

**2.登录包**

对于我们嗅探QQ密码来说。最重要的就是登录包了。在这里面包含了和QQ密码相关的信息，登录包的具体结构如下：

1. 头部

2. 初始密钥，16字节。

3. 用户的密码密钥加密的一个空串等到的16字节

4.  36字节的固定内容，未知含义

5. 登录状态， 隐身登陆 还是什么。 1字节

6. 16字节固定内容，未知含义

7.. 登录令牌长度。1字节

8. 登录令牌

9.登录模式。1字节 目前只支持普通模式

10. 未知1 字节，0x40

11. 后面段的个数，1字节 1个段9字节（猜测）

12. 段，每次基本都是固定内容，未知含义

13. 长度不足则全部填0直到符合登录包长度。UDP模式登录请求包长度为416字节

14. 尾部

其中初始密钥是一个16字节的随机数，用于本身的加密，这里最重要的就是密码密钥加密的一个空字符串，所谓密码密钥就是用QQ口令进行两次MD5加 密后得到的密文，然后以这个密文作为密钥去加密一个空字符串，这次加密使用了反馈的TEA算法，加密结果放在QQ登录包里，让服务器去验证，由于QQ的加 密算法使用特殊的填充机制使得QQ服务器可以验证出用户密码是否正确，下文会详细的解析，QQ登录包里还有一些诸如登陆状态，登录令牌和很多未知的内容。 但是对于我们破解QQ密码来说没什么大的帮助。

      QQ服务器在收到登录包之后，首先用初始密钥解密登录包后面的部分，如果解密成功，就会用保存在服务器上的QQ密码信息去解开密码密钥加密的空字符串密 文。只有当用户提交的密码正确后，解密才能成功，否则解密函数返回空，认证失败。当验证QQ客户端密码准确无误后，将返回一个登录成功包，格式如下：

 1.头部

2. 回复码，1字节

3. 会话密钥， 16字节

4. 用户的QQ号。4字节

5. 用户的IP 4字节

6. 用户的端口 2字节

7. 服务器的IP  4字节

8. 服务器的端口  2字节

9. 本次登录时间 4字节。

10. 未知 的26字节

11. 未知的服务器1 的IP ，服务器的作用未知，4字节

12.未知服务器1的端口 ，2字节

13.未知服务器2的IP 。4字节

14. 未知服务器的端口，2字节

15.2 个未知字节

16. 2个未知字节

17. Client Key ，32字节

18. 12个未知字节

 19 . 上次登录的IP 4 字节

20 .  上次登录的时间 。4字节

21. 8个未知字节

22. 尾部

我们可以看到其中包含了会话密钥，登录时间，IP ，Client  Key等内容，这些都是会在后面的具体应用中被QQ 客户端使用到。这个返回包也好似用密钥加密的。

**QQ加密算法**

了解了QQ登录的通信协议后还不足以破解QQ密码。我们还需要掌握QQ的加密算法。前面提到了，密码密钥是用户密码进行两次MD5加密之后得到的结 果。然后再用它作为密钥使用TEA算法进行加密。TEA是Tiny Encrypt Arithmetic的缩写 ，顾名思义就是一种比较简单的小型加密算法。它用一个16字节的密钥去加密一个8字节的明文，得到一个8字节的密文。也可以反向从密文解密出明文。具体的 算法可以到网上搜索查阅，这里就不再多说了。

    QQ使用的TEA虽然是标准的TEA，但是却使用了一种特殊的填充反馈机制。QQ消息被分为多个加密单元。每一个加密单元都是8字节，使用TEA进行加 密，加密结果再作为下一个单元的密钥。如果明文本身的长度不是8的倍数，那么还要进行填充，使其成为8的倍数，填充的时候会用一个32位随机数存放于明文 的开始位置，然后在明文的最后用0填充。保证整个长度是8的倍数。因为会向后反馈，这样几时对于相同的明文，因为使用不同的随机数，也会产生完全不同的密 文。

   使用这种特殊的填充反馈算法所导致的结果就是，一段密文只能用加密的密钥进行解密，如果使用不正确的密钥。就无法得到正确的填充结果。最常见的就是解密后 得到的填充数值不是0。这样就判断解密失败，服务器正式根据这种机制来确定客户端的密码是否正确的。这也是我们破解QQ密码的原理所在。

**穷举破解QQ密码**

 看到这里聪明的读者一定明白该如何通过抓包来破解QQ密码，让我们来回顾一下：

   当处于同一个局域网中的QQ客户端登录的时候，它会向服务器发送一个请求登录令牌包 ，服务器也会返回登录令牌包。但这对我们作用不大，然后他会发送登录包，里面包含了用密码密钥加密的16位密文。服务器接到登陆包后验证用户密码正确与 否，然后返回登录成功或者失败的应答包。

     我们只要抓到QQ客户端向服务端发送的登录包。先用初始密钥把他解开。就可以得到其密码密钥加密的16位密文，这样是使用同样的解密算法就能发现哪个密码 能够解开此密文。由于抓包后是本地进行破解的。只要我们的cpu够快，内存够多。破解时间够长，就一定能破出他的密码。这比通常的网络进行破解的方法要快 很多。

     有了思路。只要写出程序就可以实现QQ密码的破解里。首先是抓包。我使用里WinPcap 来抓包，这样在HUB环境下可以抓到所以的QQ包。在交换环境中，我们可以使用一些ARP欺骗工具，同样能抓到特定IP所发出的包。QQ的加密算法实现， 参考网上的Perl-oicq和LumaQQ等代码也可以轻易实现。然后用字典或者暴力破解的方法对密文进行解密即可，解密的过程用伪代码表示如下：

结果= decrypt （密文， MD5 （MD5 （密码）））

注意 ：结果不为空的时候就是正确的密码。

**QQ协议研究1 -- 基于HTTP的QQ协议研究**

2011-07-24 20:06:43|  分类： [.NET](http://yunfei3431.blog.163.com/blog/#m=0&t=1&c=fks_084064086095083068085081094095085087084065080082084065081)|字号 订阅

QQ的HTTP服务器只接受POST请求。

1.登录

 在登录协议中，QQ的密码是用标准的MD5来进行加密，DELPHI的用户只需要下个MD5加密模块就可以了。

传入协议：

 VER=1.1&CMD=Login&SEQ=&UIN=&PS=&M5=1&LC=9326B87B234E7235

 VER是用来说明QQ协议的版本

 CMD是说明协议的命令，Login就是指QQ的登录了

 SEQ是为了防止重复发送而设定的一个标记，一般我们取当前时间数值的一段放入即可

 UIN是说明你当前要登录的用户QQ号

 PS是MD5加密过后的密码的值

返回协议：

 VER=1.1&CMD=Login&SEQ=11281&UIN=&RES=0&RS=0&HI=60&LI=300（成功）

 RES为0表示成功返回

 RS为0表示登录成功

 VER=1.1&CMD=Login&SEQ=11422&UIN=315103947&RES=0&RS=1&RA=登录失败

 RS为1表示登录失败，那么就会出现提示信息RA说明原因

2.获得好友列表

得到好友名单的协议：

 VER=1.1&CMD=List&SEQ=&UIN=&TN=160&UN=0

如果成功则返回：

 VER=1.1&CMD=LIST&SEQ=43661&UIN=29501213&RES=0&FN=1&SN=24&UN=561256,1943497,....

 UN后面则是您好友的QQ号码，每个号码都由,进行分开。

3.获得QQ好友在线名单

协议如下：

 VER=1.1&CMD=Query\_Stat&SEQ=&UIN=&TN=50&UN=0

如果成功则返回：

VER=1.1&CMD=QUERY\_STAT&SEQ=-1&UIN=29501213&RES=0&FC=141,270,270,&FN=1&SN=3&ST=10,10,10,&UN=1

2327207,24259132,29501213,&NK= □,微程,鶹鸑,&

 FC为QQ头像的的ID，如的头像ID为270，那么其头使用的图片为91.bmp,其算法为ID/3+1。

 ST为QQ用户的状态，10为上线，20为离线，30为忙碌。

 UN为在线用户的QQ号

 NK为在线用户的QQ昵称。

 ST，UN，NK，每个逗号隔开的数据相互对应。

4.获得用户的详细信息

协议如下：

 VER=1.1&CMD=GetInfo&SEQ=&UIN=&LV=2&UN=

 UN为要查看用户信息的QQ号

如果成功则返回：

 VER=1.1&CMD=GETINFO&SEQ=12707&UIN=415103947&RES=0&AD=云南昆明&AG=0&EM=Microprogramer@hotmail.com&FC=270&HP=msger.org(建设中...)&JB=程序员&LV=2&PC=650000&PH=0871-6466529&PR=网络为媒%252c关系为本%252c信息为财%252c客户为主.%0d%0a&PV=云南省&RN=刘X&SC=社会大学&SX=0&UN=24259132&NK=微程

 AD用户的联系地址，AG为用户年龄，EM为用户MAIL，FC为用户头像，HP为用户网站，JB为用户职业，PC为用户邮编，PH为用户联系电话，PR为用户简介，PV为用户所以的省，RN为用户真实名称，SC为用户毕业院校，SX为用户性别，UN为用户QQ号，NK为用户QQ昵称。在得到消息后如果用的是DELPHI语言，那么要用Utf8ToAnsi()进行转换，不然会出现乱码。

5.增加好友

协议如下：

 VER=1.1&CMD=AddToList&SEQ=&UIN=&UN=

 UN为我们要增加用户的QQ号

如果成功则返回：  
 VER=1.1&CMD=AddToList&SEQ=13666&UIN=415103947&RES=0&CD=0&UN=24259132

 CD为被加QQ的身份验证状态，CD为0表示“允许任何人把我列为好友”，CD为1表示“需要身份证认才能把我列为好友”，CD为3表示“不允许任何人把我列为好友”。如果CD为0那么信息回馈后，用户就直接加为好友了，如果CD为1，那么还要发送一次回应加为好友的响应

6.回应加为好友的响应

 回应加为好友响应是双方的：1、如果你发送了请求加对方为好友，如果对方需要验证，那么必需发送回应加为好友的响应。2、如果对方发送加为好友请求给你，那么你可以发送加为好友的响应，一是加为好友，一是通过验证，一是拒决加为好友。我们要向服务器发送命令：

 VER=1.1&CMD=Ack\_AddToList&SEQ=&UIN=&UN=&CD=&RS=

 CD为响应状态，CD为0表示“通过验证”。CD为1表示“拒决加为对方为好友”。CD为2表示“请求对方加为好友”。

 RS为你要请求的理由。

服务器得到协议后如果成功则返回：

 VER=1.1&CMD=Ack\_AddToList&SEQ=1130&UIN=415103947&RES=0&

7.删除好友

向服务器发送DelFromList命令则可以删除用户：

 VER=1.1&CMD=DelFromList&SEQ=&UIN=&UN=

 UN为要删除用户的QQ号

如果成功则返回：

 VER=1.1&CMD=DelFromList&SEQ=24514&UIN=415103947&RES=0&

8.改变用户当前状态

具体命令如下：

 VER=1.1&CMD=Change\_Stat&SEQ=&UIN=&ST=

 ST为要改变的状态，10为上线，20为离线，30为忙碌。

如果成功则返回：

 VER=1.1&CMD=Change\_Stat&SEQ=17512&UIN=415103947&RES=0&

9.退出

具体命令如下：

 VER=1.1&CMD=Logout&SEQ=&UIN=

如果成功则返回：

 VER=1.1&CMD=LOGOUT&SEQ=15803&UIN=415103947&RES=0

10.获得好友的消息

具体命令如下：

 VER=1.1&CMD=GetMsgEx&SEQ=&UIN=

如果成功则返回：

 VER=1.1&CMD=GETMSGEX&SEQ=56661&UIN=29501213&RES=0&MN=3&MT=99,9,9,&UN=24259132,24259132,24259132,&MG=30 ,asdfasdfasdfasdf ,asdfasdfasdf ,&

 MT表示消息类型，99表示系统消息，9表示用户消息

 UN表示消息发送来源用户

 MG表示发送的消息，MG消息可以表示某些特定的系统含意，譬如：当MT为99，MG为30，UN为24259132则表示用户4259132现在处于忙碌状态，可根据此消息进行好友列表的刷新，提高效率

11.向好友发送消息

具体命令如下：

 VER=1.1&CMD=CLTMSG&SEQ=&UIN=&UN=&MG=  
 UN为消息发送给的用户QQ号码

 MG为发送给该用户的消息

如果成功则返回：

 VER=1.1&CMD=CLTMSG&SEQ=15803&UIN=415103947&RES=0

### QQ密码破解原理

2011-02-26 14:58:28|  分类： [默认分类](http://chengxinmimawang.blog.163.com/blog/#m=0&t=1&c=fks_084065086087087068083082087095085094080066080085082074083)|字号 订阅

今天给大家带来的是 [QQ密码破解](http://www.pojiemima.net/)原理，这也是很多学员怀疑的地方，导致很多不相信我们是否能破解别人的QQ密码，今天我会给大家解释一下。

                 简介：QQ密码破解教程在网上很多，五花八门，看多了越来越头痛．导致有很多朋友都被误导，＂QQ密码破解的配置真他妈的难＂.....今天我本人对QQ密码破解原理进行讲解一下．

QQ密码在正确登陆后，会将加密的结果保存在用户目录的ewh.db文件中，加密采用公开的MD5算法，通过N次循环以及异或后求反，最终计算出加密的结果，与用户的ewh.db文件中的密文比较后，发出"输入密码与上次成功登录的密码不一致,$0A是否到服务器验证?"（这条信息在BasicCtrlDll.dll的资源中，$0A在C的格式化中为回车）。根据这个提示，完成本地QQ密码的暴力破解。

　　在QQ系统中，"QD"标志代表QQ Data，例如，我们可以在文件User.db或ewh.db中找到这个以QD开头的数据结构。

　　一、 ewh.db原始数据

　　51 44 01 01 03 00 04 03 00 BD AF A8 04 00 00 00

　　00 2E 06 00 07 03 00 B9 AB B4 10 00 00 00 07 22

　　AA 96 56 19 A3 9E 82 19 B7 2B BD 2D 34 4A 04 03

　　00 A9 B5 B2 04 00 00 00 3C A8 93 06

　　其中，红色为AST循环次数，兰色为EWH加密字符串，绿色为UIN QQ号（110340156=0x0693A83C，Intel体系内存中排列顺序为：3CA89306）。

　　二、 ewh.db数据结构

　　HEX

　　偏移 DEC

　　偏移 数据 注释 变量

　　标志

　　0000 1 51 44 QD，QQ Data 数据标志 Flag

　　0002 3 01 01 保留的数据结构 Reserve

　　0004 5 03 00 总数据段（Data Sections）的个数 Sections

　　0006 7 04 第一个数据段（简称1S，下同）的类型，可以从0x01到0x0F，04代表本数据没经过加密处理。 Type1S

　　0007 8 03 00 1S标志的长度。 LenFlag1S

　　0009 10 BD AF A8 1S标志（例如AST、UIN、EWH等），是经过简单的异或并求反计算处理的，此处是AST，可能是Algorithm Shift Times 或Axxx Switch Time，管他的呢！ Flag1S

　　000C 13 04 00 00 00 1S数据的长度 LenData1S

　　0010 17 00 2E 06 00

　　= (404992) 1S数据，这里是进行MD5转换的次数。

　　这个数据是同计算机的性能有关的，性能越高的计算机，在QQ注册成功后产生的这个循环控制变量就越大。 Data1S

　　0014 21 07 2S数据的类型，07代表使用MD5进行加密 Type2S

　　0015 22 03 00 2S标志的长度 LenFlag2S

　　0017 24 B9 AB B4 2S标志，此处是EWH，代表本数据段是EWH密码数据，可能是Encrypt With Hash的缩写 Flag2S

　　001A 27 10 00 00 00 2S数据的长度 LenData2S

　　001E 31 07 22 AA 96

　　56 19 A3 9E

　　82 19 B7 2B

　　BD 2D 34 4A 2S数据，是经过MD5加密计算后产生的数据，当然还要经过异或并求反的计算处理，参考下面程序中的1000B858 行代码。 Data2S

　　002E 47 04 3S数据的类型 Type3S

　　002F 48 03 00 3S标志的长度 LenFlag3S

　　0031 50 A9 B5 B2 3S标志，此处是UIN，代表本数据段是QQ号码，可能是：User Identifier Number的缩写 Flag3S

　　0034 53 04 00 00 00 3S数据的长度 LenData3S

　　0038 57 3C A8 93 06 3S数据，3C A8 93 06 = 110340156 Data3S

　　三、 加密原理

　　下面VB伪代码的部分符号引自以上第二点《结构说明》中的变量标志，请注意理解：

　　Pwd = MD5(Pwd, Len(Pwd))

　　' Pwd为用户输入的密码，第一轮MD5后，Pwd成为16位字节长度的MD5串。

　　XorKey As Long = 0 'XorKey为用于解密的字节

　　For k = 1 To Data1S - 1 '因为前面已经做过一轮，所以此处要减一

　　Pwd = MD5(Pwd, 16)

　　Next k

　　XorKey = XorKey And &HFFFF

　　XorKey = (LenData2S And &HFF) Xor (LenData2S \ 256)

　　XorKey = &HFF - XorKey '求反

　　For k = 1 To 16

　　Pwd(k) = Pwd(k) Xor XorKey

　　Next k

　　If Pwd <> Data2S Then

　　MsgBox "输入密码与上次成功登录的密码不一致," & vbcrlf & "是否到服务器验证?"

　　End If

　　通过以上的流程，我真的佩服QQ的设计者，如此巨大的循环量，加上循环次数的随机性，如果希望产生一个QQ MD5词典简直不可能。虽然理论上，可以产生一个MD5字典，但是，这个字典将有1.15E+77\*16个字节之巨，因此，只好根据ewh.db文件提供的数据暴力破解了，不知是不是有更好的方法呢？

　　不过我的感觉是，循环次数加多了，应该会产生更多的MD5碰撞，不见得是个好事。

　　还有一种破解思路，也许更加直接，将在后面的文章中详细探讨。但是我只有在有时间做完实验后才有资格评述，不在本文章的讨论范围内。

　　四、 破解算法

　　重复进行数十万次MD5加密，会消耗计算机很多时间，如果使用传统的VB或VC，对于一个密码的等待时间也是很可观的（例如使用VB代码，消耗的时间可能是汇编的400倍），因此，我使用汇编语言来编制低层加密解密算法，通过MASM32编译连接，最后用高级语言调用。通过提供算法动态库的方式，方便其他有兴趣的读者自己增加丰富的功能。例如增加多线程等，这也将在以后的探讨中实现。在此不做深入讨论。

　　附带的例子为VB和VC调用汇编语言动态库的例子，VB代码简单实现了通过密码字典进行单线程破解的功能，读者可以丰富其内容。增加更多的功能。

五、 QQ数据结构分析

　　下面为动态库BasicCtrlDll.dll中反汇编的代码以及代码分析，主要用于分析EWH.DB中数据结构以及QQ数据解调算法的问题。另外，这个算法也可以将User.db中的数据提取出来。深入研究下去，做一个聊天记录查看器之类的软件也非难事。

　　1000B71D B8 AC160110 mov eax,BasicCtr.100116AC

　　1000B722 E8 89460000 call BasicCtr.1000FDB0

　　1000B727 83EC 3C sub esp,3C

　　1000B72A 8B45 08 mov eax,dword ptr ss:[ebp+8] 将数据的开始地址赋给EAX，实际数据为\*\*Data，EAX=\*Data

　　1000B72D 53 push ebx

　　1000B72E 56 push esi

　　1000B72F 57 push edi

　　1000B730 8B30 mov esi,dword ptr ds:[eax] 需要转换的字符串，EAX指示一个结构，第一个成员为实际的数据指针

　　1000B732 894D D8 mov dword ptr ss:[ebp-28],ecx 局部变量[ebp-28]保存全局的标志结构，ECX为全局参数地址，在调用本函数时跟入

　　1000B735 8B46 F8 mov eax,dword ptr ds:[esi-8] 为CString结构中长度的成员，表示总共多少个字节

　　1000B738 83F8 06 cmp eax,6 如果长度小于6，则为无效的数据

　　1000B73B 0F82 81020000 jb BasicCtr.1000B9C2 如果比6小则跳转退出，说明数据量不够解调的

　　1000B741 803E 51 cmp byte ptr ds:[esi],51 是否为 QQ Data 的数据，QD为QQ数据标志

　　1000B744 0F85 78020000 jnz BasicCtr.1000B9C2

　　1000B74A 807E 01 44 cmp byte ptr ds:[esi+1],44

　　1000B74E 0F85 6E020000 jnz BasicCtr.1000B9C2

　　1000B754 66:8B7E 04 mov di,word ptr ds:[esi+4] 对于EWH来说，为第4+1个字节，为0003

　　1000B758 83C6 04 add esi,4 指向数据段(Sections)的个数

　　1000B75B 46 inc esi

　　1000B75C 83C0 FA add eax,-6 EAX去掉6个字节，对于EWH来说，剩下36H个字节

　　1000B75F 46 inc esi

　　1000B760 8945 08 mov dword ptr ss:[ebp+8],eax 指向第一个数据段

　　1000B763 E8 CE050000 call BasicCtr.1000BD36 在内存（ECX+9C）处开辟一个(100H)字节的空间，空间地址返回到EAX

　　1000B768 8365 E0 00 and dword ptr ss:[ebp-20],0 局部变量[ebp-20]清零

　　1000B76C 0FB7C7 movzx eax,di 转换到EAX，对于EWH，di=3。表示有3段数据

　　1000B76F 85C0 test eax,eax

　　1000B771 8945 B8 mov dword ptr ss:[ebp-48],eax 局部变量[ebp-48]保存数据的段数

　　1000B774 0F8E 21020000 jle BasicCtr.1000B99B

　　1000B77A 837D 08 07 cmp dword ptr ss:[ebp+8],7 如果整个长度小于7，则剩下的应该是QQ号了。第一次进入时=36H

　　1000B77E 0F82 3E020000 jb BasicCtr.1000B9C2 如果剩余的数据长度小于7则退出

　　1000B784 8A06 mov al,byte ptr ds:[esi] 第一次进入时，ESI指向第7个数据即数据段的类型，例如 04

　　1000B786 66:8B4E 01 mov cx,word ptr ds:[esi+1] CX=后一个数据，及数据段标志的长度，例如 0003

　　1000B78A 46 inc esi

　　1000B78B 8B55 08 mov edx,dword ptr ss:[ebp+8] 剩余的数据长度，如36H

　　1000B78E 836D 08 03 sub dword ptr ss:[ebp+8],3 去掉3个，例如成为33H=51

　　1000B792 894D C8 mov dword ptr ss:[ebp-38],ecx 局部变量[ebp-38]保存数据段中标志长度

　　1000B795 0FB7F9 movzx edi,cx EDI为标志长度了

　　1000B798 46 inc esi

　　1000B799 8845 E4 mov byte ptr ss:[ebp-1C],al 局部变量[ebp-1C]保存本段的类型

　　1000B79C 8D4F 04 lea ecx,dword ptr ds:[edi+4] ECX为取得的标志长度再加上4，例如=7

　　1000B79F 46 inc esi 第一次时，ESI指向第一个数据段的标志字段了，例如指向BDAFA8，第9个数据开始

　　1000B7A0 394D 08 cmp dword ptr ss:[ebp+8],ecx 如果剩余的数据比"标志长度+4"还少，则没有数据，因此不进行处理

　　1000B7A3 0F82 19020000 jb BasicCtr.1000B9C2

　　1000B7A9 8B0C37 mov ecx,dword ptr ds:[edi+esi] 跳过数据段的标志部分，将数据段的长度赋值给ECX。例如[edi+esi]=4

　　1000B7AC 8D1C37 lea ebx,dword ptr ds:[edi+esi] EBX保存新的指针，指向数据段中数据部分的长度部分，例如，[EBX]=4

　　1000B7AF 895D C4 mov dword ptr ss:[ebp-3C],ebx 局部变量[ebp-3C]保存数据段中数据部分的长度指针

　　1000B7B2 8D4C0F 07 lea ecx,dword ptr ds:[edi+ecx+7] 从标志（自身长3，加上4个长度位=7）开始，加上数据长度，为完整数据长度。例如E

　　1000B7B6 3BCA cmp ecx,edx 如果剩下的数据长度（如36H）不够，则退出

　　1000B7B8 894D CC mov dword ptr ss:[ebp-34],ecx 局部变量[ebp-34]保存本数据段的总长度

　　1000B7BB 0F87 01020000 ja BasicCtr.1000B9C2 如果小于则退出程序

　　1000B7C1 8365 F0 00 and dword ptr ss:[ebp-10],0 局部变量[ebp-10]清零

　　1000B7C5 3C 01 cmp al,1 al保存本段的类型，有效的类型是4或7

　　1000B7C7 74 18 je short BasicCtr.1000B7E1

　　1000B7C9 3C 02 cmp al,2

　　1000B7CB 74 14 je short BasicCtr.1000B7E1

　　1000B7CD 3C 03 cmp al,3

　　1000B7CF 74 10 je short BasicCtr.1000B7E1

　　1000B7D1 3C 04 cmp al,4

　　1000B7D3 74 0C je short BasicCtr.1000B7E1

　　1000B7D5 3C 05 cmp al,5

　　1000B7D7 74 08 je short BasicCtr.1000B7E1

　　1000B7D9 3C 07 cmp al,7

　　1000B7DB 74 04 je short BasicCtr.1000B7E1

　　1000B7DD 3C 06 cmp al,6

　　1000B7DF 75 19 jnz short BasicCtr.1000B7FA

　　1000B7E1 51 push ecx 为本段的总长度，包括（段类型+标志长度+标志+数据长度+数据），例如，对于密码段=1AH

1000B7E2 E8 23430000 call

　　1000B7E7 FF75 CC push dword ptr ss:[ebp-34] n=[ebp-34]，局部变量[ebp-34]保存本数据段的总长度

　　1000B7EA 8D4E FD lea ecx,dword ptr ds:[esi-3] [esi-3]指向本段的开始（从段类型算起）

　　1000B7ED 8945 F0 mov dword ptr ss:[ebp-10],eax 局部变量[ebp-10]保存拷贝后的数据

　　1000B7F0 51 push ecx src

　　1000B7F1 50 push eax dest

　　1000B7F2 E8 E5450000 call memcpy，将本段的整段数据拷贝到新的地方，数据指针保存在局部变量[ebp-10]中

　　1000B7F7 83C4 10 add esp,10

　　1000B7FA 8B45 C8 mov eax,dword ptr ss:[ebp-38] 局部变量[ebp-38]保存数据段中标志长度

　　1000B7FD 33C9 xor ecx,ecx

　　1000B7FF 32C4 xor al,ah 将低位长度与高位异或，例如3 xor 0=3

　　1000B801 85FF test edi,edi EDI为标志位的长度

　　1000B803 76 12 jbe short BasicCtr.1000B817 如果本段没有段标志，则跳转

　　1000B805 8A1431 mov dl,byte ptr ds:[ecx+esi] 开始循环，循环次数为标志的长度。ECX第一次时为0，将第一个数据加载到DL中。

　　1000B808 32D0 xor dl,al AL为长度的高位和低位的异或，这里为3

　　1000B80A F6D2 not dl DL=NOT ([数据] xor [数据段标志长度的高位 xor 数据段标志长度的低位])

　　1000B80C 881431 mov byte ptr ds:[ecx+esi],dl 数据保存在原始的内存中相应的地方

　　1000B80F 41 inc ecx

　　1000B810 3BCF cmp ecx,edi

　　1000B812 72 F1 jb short BasicCtr.1000B805

　　1000B814 8B5D C4 mov ebx,dword ptr ss:[ebp-3C] 局部变量[ebp-3C]保存数据段中数据部分的长度指针

　　1000B817 57 push edi EDI为标志位的长度

　　1000B818 56 push esi ESI为指向解密以后的数据，例如AST

　　1000B819 8D4D E8 lea ecx,dword ptr ss:[ebp-18] 局部变量[ebp-18]存放强制类型转换以后的数据指针的指针，例如AST

　　1000B81C E8 5B430000 call 将解密后的数据变成CString类型。返回的类型放在EAX指示的地址中

　　1000B821 8365 FC 00 and dword ptr ss:[ebp-4],0 局部变量[ebp-4]清零

　　1000B825 6A FC push -4

　　1000B827 58 pop eax EAX=-4=FFFFFFFC

　　1000B828 8BF3 mov esi,ebx ebx保存数据段中数据部分的长度指针

　　1000B82A 2BC7 sub eax,edi EAX=EAX-EDI=FFFFFFFC-3=FFFFFFF9

　　1000B82C 8B1E mov ebx,dword ptr ds:[esi] ebx为数据段中数据部分的长度了

　　1000B82E 0145 08 add dword ptr ss:[ebp+8],eax 第一次时，[EBP+8]=33。执行后=2C，相当于33H-7H=2CH

　　1000B831 83C6 04 add esi,4 ESI指向数据段中的数据部分了

　　1000B834 395D 08 cmp dword ptr ss:[ebp+8],ebx [ebp+8]=2C，ebx=4

　　1000B837 0F82 6A010000 jb BasicCtr.1000B9A7

　　1000B83D 807D E4 07 cmp byte ptr ss:[ebp-1C],7 局部变量[ebp-1C]保存本段的类型，4或者7

　　1000B841 74 06 je short BasicCtr.1000B849

　　1000B843 807D E4 06 cmp byte ptr ss:[ebp-1C],6 如果类型不为6，则执行1000B862

　　1000B847 75 19 jnz short BasicCtr.1000B862

　　1000B849 8AC3 mov al,bl 如果数据段的类型为7，则执行此语句。BL包含本段的长度

　　1000B84B 33FF xor edi,edi

　　1000B84D 32C7 xor al,bh al=（长度的低位 xor 长度的高位）

　　1000B84F 85DB test ebx,ebx

　　1000B851 76 0F jbe short BasicCtr.1000B862 如果长度为0，则表示没有密码

　　1000B853 8A0C37 mov cl,byte ptr ds:[edi+esi]

　　1000B856 32C8 xor cl,al

　　1000B858 F6D1 not cl DL=NOT ([数据] xor [数据段标志长度的高位xor 数据段标志长度的低位])

　　1000B85A 880C37 mov byte ptr ds:[edi+esi],cl

　　1000B85D 47 inc edi

　　1000B85E 3BFB cmp edi,ebx

　　1000B860 72 F1 jb short BasicCtr.1000B853 循环直到全部数据解调完毕

　　1000B862 53 push ebx 数据串的长度

　　1000B863 56 push esi 原始的需要变换的数据

　　1000B864 8D4D EC lea ecx,dword ptr ss:[ebp-14] 局部变量[ebp-14]存放强制CString类型转换以后的数据指针的指针，例如DB2E0600

　　1000B867 E8 10430000 call

　　1000B86C 8A45 E4 mov al,byte ptr ss:[ebp-1C] 局部变量[ebp-1C]保存本段的类型，4或者7

　　1000B86F 295D 08 sub dword ptr ss:[ebp+8],ebx 去掉已经处理的数据，执行后[ebp+8]=28H，ebx为数据段中数据部分的长度

　　1000B872 03F3 add esi,ebx ESI指向下一个数据段的开始部分，ebx保存数据段中数据部分的长度指针

　　1000B874 33FF xor edi,edi

　　1000B876 84C0 test al,al 测试本段的类型是否为0

　　1000B878 C645 FC 01 mov byte ptr ss:[ebp-4],1 局部布尔型变量[ebp-4]=1

　　1000B87C 0F86 A3010000 jbe BasicCtr.1000BA25 如果本段的数据类型为0，则执行1000BA25后退出

　　1000B882 3C 07 cmp al,7

　　1000B884 0F86 B6000000 jbe BasicCtr.1000B940 如果小于等于7，则跳转到1000B940执行。对于EWH来说就是这样

　1000B88A 3C 08 cmp al,8

　　1000B88C 0F84 74010000 je BasicCtr.1000BA06 如果数据类型为8，则直接退出。

　　1000B892 3C 09 cmp al,9

　　1000B894 74 5D je short BasicCtr.1000B8F3

　　1000B896 3C 0A cmp al,0A

　　1000B898 0F85 87010000 jnz BasicCtr.1000BA25

　　1000B89E 8B4D D8 mov ecx,dword ptr ss:[ebp-28] 当数据类型为A时，执行本程序代码

　　1000B8A1 8D45 D4 lea eax,dword ptr ss:[ebp-2C]

　　1000B8A4 50 push eax

　　1000B8A5 E8 47FEFFFF call BasicCtr.1000B6F1

　　1000B8AA 8B45 D4 mov eax,dword ptr ss:[ebp-2C]

　　1000B8AD FF75 EC push dword ptr ss:[ebp-14]

　　1000B8B0 8B08 mov ecx,dword ptr ds:[eax]

　　1000B8B2 53 push ebx

　　1000B8B3 50 push eax

　　1000B8B4 FF91 BC000000 call dword ptr ds:[ecx+BC]

　　1000B8BA 8BD8 mov ebx,eax

　　1000B8BC 85DB test ebx,ebx

　　1000B8BE 0F85 12010000 jnz BasicCtr.1000B9D6

　　1000B8C4 8B45 D4 mov eax,dword ptr ss:[ebp-2C]

　　1000B8C7 6A 04 push 4

　　1000B8C9 8945 DC mov dword ptr ss:[ebp-24],eax

　　1000B8CC 8D45 DC lea eax,dword ptr ss:[ebp-24]

　　1000B8CF 50 push eax

　　1000B8D0 8D4D C0 lea ecx,dword ptr ss:[ebp-40]

　　1000B8D3 E8 A4420000 call

　　1000B8D8 50 push eax

　　1000B8D9 8D4D EC lea ecx,dword ptr ss:[ebp-14]

　　1000B8DC C645 FC 03 mov byte ptr ss:[ebp-4],3

　　1000B8E0 E8 C3400000 call

　　1000B8E5 C645 FC 01 mov byte ptr ss:[ebp-4],1

　　1000B8E9 8D4D C0 lea ecx,dword ptr ss:[ebp-40]

　　1000B8EC E8 AB400000 call

　　1000B8F1 EB 50 jmp short BasicCtr.1000B943

　　1000B8F3 8B4D D8 mov ecx,dword ptr ss:[ebp-28] 当数据类型为9时，执行这个操作

　　1000B8F6 8D45 D0 lea eax,dword ptr ss:[ebp-30]

　　1000B8F9 50 push eax

　　1000B8FA E8 4E180000 call BasicCtr.1000D14D

　　1000B8FF 8B45 D0 mov eax,dword ptr ss:[ebp-30]

　　1000B902 FF75 EC push dword ptr ss:[ebp-14]

　　1000B905 8B08 mov ecx,dword ptr ds:[eax]

　　1000B907 53 push ebx

　　1000B908 50 push eax

　　1000B909 FF51 78 call dword ptr ds:[ecx+78]

　　1000B90C 8BD8 mov ebx,eax

　　1000B90E 85DB test ebx,ebx

　　1000B910 0F85 D4000000 jnz BasicCtr.1000B9EA

　　1000B916 8B45 D0 mov eax,dword ptr ss:[ebp-30]

　　1000B919 6A 04 push 4

　　1000B91B 8945 DC mov dword ptr ss:[ebp-24],eax

　　1000B91E 8D45 DC lea eax,dword ptr ss:[ebp-24]

　　1000B921 50 push eax

　　1000B922 8D4D BC lea ecx,dword ptr ss:[ebp-44]

　　1000B925 E8 52420000 call

　　1000B92A 50 push eax

　　1000B92B 8D4D EC lea ecx,dword ptr ss:[ebp-14]

　　1000B92E C645 FC 02 mov byte ptr ss:[ebp-4],2

　　1000B932 E8 71400000 call

　　1000B937 C645 FC 01 mov byte ptr ss:[ebp-4],1

　　1000B93B 8D4D BC lea ecx,dword ptr ss:[ebp-44]

　　1000B93E EB AC jmp short BasicCtr.1000B8EC

　　1000B940 6A 01 push 1 当数据段的类型<=7时，直接从此处执行

　　1000B942 5F pop edi

　　1000B943 8B5D D8 mov ebx,dword ptr ss:[ebp-28] 局部变量[ebp-28]保存全局的标志结构

　　1000B946 8D45 EC lea eax,dword ptr ss:[ebp-14] 局部变量[ebp-14]存放强制类型转换以后的数据指针的指针，例如DB2E0600

1000B949 50 push eax EAX存放强制类型转换以后的数据指针

　　1000B94A 8D45 E8 lea eax,dword ptr ss:[ebp-18] 局部变量[ebp-18]存放强制类型转换以后的数据指针的指针，例如AST

　　1000B94D FF75 E4 push dword ptr ss:[ebp-1C] 局部变量[ebp-1C]中的第一个字节保存本段的类型，4或者7

　　1000B950 8BCB mov ecx,ebx

　　1000B952 50 push eax

　　1000B953 E8 B4FCFFFF call BasicCtr.1000B60C call 1000B60C(CString,Flag,CString)

　　1000B958 85FF test edi,edi

　　1000B95A 74 18 je short BasicCtr.1000B974

　　1000B95C 8B45 E0 mov eax,dword ptr ss:[ebp-20] 局部变量[ebp-28]第一次为0，为一个计数器

　　1000B95F 8B4B 64 mov ecx,dword ptr ds:[ebx+64] 存在于标志结构中，为一个全局地址

　　1000B962 8B55 F0 mov edx,dword ptr ss:[ebp-10] 局部变量[ebp-10]保存拷贝后的数据，即没有经过处理的。例如040300BDAF......

　　1000B965 C1E0 02 shl eax,2 EAX=EAX\*2

　　1000B968 891401 mov dword ptr ds:[ecx+eax],edx 将未做解调的原始数据放到全局结构中某个指针指示的内存中

　　1000B96B 8B4B 78 mov ecx,dword ptr ds:[ebx+78] 存在于标志结构中，为一个全局地址

　　1000B96E 8B55 CC mov edx,dword ptr ss:[ebp-34] 局部变量[ebp-34]保存本数据段的总长度

　　1000B971 891401 mov dword ptr ds:[ecx+eax],edx 将数据长度放到全局结构中某个指针指示的内存中

　　1000B974 8065 FC 00 and byte ptr ss:[ebp-4],0 局部布尔型变量[ebp-4]=0

　　1000B978 8D4D EC lea ecx,dword ptr ss:[ebp-14]

　　1000B97B E8 1C400000 call 清除数据段中的数据部分CString

　　1000B980 834D FC FF or dword ptr ss:[ebp-4],FFFFFFFF 局部布尔型变量[ebp-4]=-1，为True

　　1000B984 8D4D E8 lea ecx,dword ptr ss:[ebp-18]

　　1000B987 E8 10400000 call 清除数据段中的标志部分CString，例如AST

　　1000B98C FF45 E0 inc dword ptr ss:[ebp-20] 局部变量[ebp-28]计数器加一

　　1000B98F 8B45 E0 mov eax,dword ptr ss:[ebp-20]

　　1000B992 3B45 B8 cmp eax,dword ptr ss:[ebp-48] 局部变量[ebp-48]保存数据的段数

　　1000B995 0F8C DFFDFFFF jl BasicCtr.1000B77A 循环解调每个数据段

　　1000B99B 8B45 08 mov eax,dword ptr ss:[ebp+8] 最后剩余的长度

　　1000B99E F7D8 neg eax

　　1000B9A0 1BC0 sbb eax,eax

　　1000B9A2 83E0 04 and eax,4

　　1000B9A5 EB 1E jmp short BasicCtr.1000B9C5

　　1000B9A7 837D F0 00 cmp dword ptr ss:[ebp-10],0

　　1000B9AB 74 09 je short BasicCtr.1000B9B6

　　1000B9AD FF75 F0 push dword ptr ss:[ebp-10]

　　1000B9B0 E8 FF3F0000 call

　　1000B9B5 59 pop ecx

　　1000B9B6 834D FC FF or dword ptr ss:[ebp-4],FFFFFFFF

　　1000B9BA 8D4D E8 lea ecx,dword ptr ss:[ebp-18]

　　1000B9BD E8 DA3F0000 call

　　1000B9C2 6A 04 push 4

　　1000B9C4 58 pop eax

　　1000B9C5 8B4D F4 mov ecx,dword ptr ss:[ebp-C]

　　1000B9C8 5F pop edi

　　1000B9C9 5E pop esi

　　1000B9CA 5B pop ebx

　　1000B9CB 64:890D 000000 mov dword ptr fs:[0],ecx

　　1000B9D2 C9 leave

　　1000B9D3 C2 0400 retn 4

　　1000B9D6 837D F0 00 cmp dword ptr ss:[ebp-10],0

　　1000B9DA 74 09 je short BasicCtr.1000B9E5

　　1000B9DC FF75 F0 push dword ptr ss:[ebp-10]

　　1000B9DF E8 D03F0000 call

　　1000B9E4 59 pop ecx

　　1000B9E5 8B45 D4 mov eax,dword ptr ss:[ebp-2C]

　　1000B9E8 EB 12 jmp short BasicCtr.1000B9FC

　　1000B9EA 837D F0 00 cmp dword ptr ss:[ebp-10],0

　　1000B9EE 74 09 je short BasicCtr.1000B9F9

　　1000B9F0 FF75 F0 push dword ptr ss:[ebp-10]

　　1000B9F3 E8 BC3F0000 call

　　1000B9F8 59 pop ecx

　　1000B9F9 8B45 D0 mov eax,dword ptr ss:[ebp-30]

　　1000B9FC 8B08 mov ecx,dword ptr ds:[eax]

　　1000B9FE 50 push eax

　　1000B9FF FF51 08 call dword ptr ds:[ecx+8]

　　1000BA02 8BF3 mov esi,ebx

　　1000BA04 EB 03 jmp short BasicCtr.1000BA09

　　1000BA06 6A 04 push 4

　　1000BA08 5E pop esi

　　1000BA09 8065 FC 00 and byte ptr ss:[ebp-4],0

　　1000BA0D 8D4D EC lea ecx,dword ptr ss:[ebp-14]

　　1000BA10 E8 873F0000 call

　　1000BA15 834D FC FF or dword ptr ss:[ebp-4],FFFFFFFF

　　1000BA19 8D4D E8 lea ecx,dword ptr ss:[ebp-18]

　　1000BA1C E8 7B3F0000 call

　　1000BA21 8BC6 mov eax,esi

　　1000BA23 EB A0 jmp short BasicCtr.1000B9C5

　　1000BA25 8065 FC 00 and byte ptr ss:[ebp-4],0

　　1000BA29 8D4D EC lea ecx,dword ptr ss:[ebp-14]

　　1000BA2C E8 6B3F0000 call

　　1000BA31 EB 83 jmp short BasicCtr.1000B9B6

　　以上代码看不懂没关系，在压缩包中的VB代码 LoAnalysisQD (fbyt() As Byte) 函数概括了上述的思想，不过，对于4和7以外的数据类型，由于与本文内容无关，因此，不深入分析。

六、 QQ的另类破解

　　1、QQ密码算法和身份验证中存在的问题

　　搞个几十万次加密其实并不能阻止密码的破解，我对现在收集的EWH.db进行统计，那个循环的AST都在40万以上（可以买房子了，不是么？），因此，只要做一个40万的QQ Hash词典，在此基础上进行破解，破解速度不就提高了几万倍么？

　　这个词典如何形成？问得好！事实上，国际上有合作破解的先例。例如，可以给我分配000000000~999999999的段进行计算，给你分配999999999~1999999999的段进行计算......，最后，将所有结果合成为一个词典（或者根本不用合成，把Hash值发给大家就可以了，总有人能中大奖：）。

　　这个词典称为Hash词典，大致上是这样的（密码经过400000次加密后得到）：

　　索引（密码） Hash值（加密后的密文）

　　1 2E62CD38389C3A885D7F6789FEEE8AA5

　　2 1F9C9B12E93A0FF2A9B7A714EF4D6CA4

　　3 8FE71CEF95D0F0DDAD716651E635D19C

　　...... ......

　　999999999 A041F9E6DDA44C178F24DABC9B292785

　　有了这个Hash词典，我们完全没有必要重新忍受漫长的计算过程，直接查表就可以了，不是吗？用黑客的行话来说，就是跑字典了。

　　利用压缩包中提供的函数QQMD5(unsigned char \*, long, long, QQSum \*)，就完全可以形成这个词典了。

　　别笑，这好象是大炮打蚊子，对于一个小小的QQ来说，何必劳驾全世界呢？既然这是我们闲得无聊下来干的事，我们就该自己来做。

　　最简单的Hash词典就是利用黑客词典（网上简直多如牛毛）再通过QQMD5函数来生成，如果你想到用数据库来管理这些Hash值，你一定是个非常敬业的黑客，不过数据库也是TB级的了。

　　Hash散列算法非常容易产生碰撞，如果你偶尔发现输入12345和输入78952一样可以登录QQ，你千万不要怪腾讯公司没水平，这是因为12345和78952产生的Hash相同（别试，我随便说的两个数），这说明，一个Hash输出可能对应多个输入，这就是碰撞。听说山东大学的王教授就很擅长产生这种碰撞，强烈要求他来做我们的斑竹。

　　因为碰撞，我们的词典就会小一点，不过，这些理想和共产主义一样，离我们很远，即使王教授的快速碰撞理论，对于QQ这样的重复加密来说，只是加快计算时间，并不能对整个加密体系构成威胁，所以，即使这个世界有那么多的恐怖份子，你我夏天还是穿个短裤就可以上街。

　　况且，现在很多的及时通讯系统都采用本地和服务器联合验证的方式，这非常有效，即使本地的密码被攻破了，但是，不能保证服务器的也被攻破。因为，通过暴力方式破解的登录口令也只是众多产生碰撞的口令之一，如果使用不同的加密方式，即使这个口令能进入本地系统，但是不能保证同一个口令在服务器端得到验证。所以，QQ从这个意义上说，依然是相对安全的（不过众多口令中，可能就只有一个特别象口令）。

　　刚才提到密码算法的问题，谈到的所有问题都是本地的密码机制，对于网络之间的报文，采用的又是TEA的加密算法。这个是我后面的文章要分析的。

　　在QQ的身份验证中，还存在另外一个漏洞，这个漏洞很早就被发现了，一直保留到现在，也许将来也不会改变。

　　我不说大家也都知道，将EWH.DB中的QQ号（第一点中的那个3C A8 93 06）替换成别人的QQ号，然后把这个东西放在别人的目录下，就可以看到那个倒霉蛋的聊天记录了。不过，好在腾迅的服务器不买这个帐：看就看吧，只要我这里安全就没事了，多看点多学点，下次聊天就更欢了。

　　从低层的逻辑也可以看得出来，只要用户的EWH.DB文件符合我们前面的算法，QQ就认为这个用户是合法的。因此，我们完全可以想象，如果我自己做一个EWH.DB文件，让那个40万次的东西变成0，岂不是可以让我的计算机从那个傻呼呼的循环中解脱出来吗？更懒的人可能想到，如果不用密码岂不是更爽？好，我们来实现这个愿望：

　　运行QQPwdFinality.exe，将登录口令中的"12345"删掉，将"循环次数"改为0，进行单步计算后，是不是得到了一个串？如果你的计算机没骗你的话，大家应该都得到同一个结果：

3BF2633660EF5DEB066FE6770317AD91，好了，我们将这个结果替换掉EWH.DB中的那个Hash值07 22 AA 96 56 19 A3 9E 82 19 B7 2B BD 2D 34 4A，最后，EWH.DB文件变成下面这个样子（记得将循环次数也改成0哦）：

　　51 44 01 01 03 00 04 03 00 BD AF A8 04 00 00 00

　　00 00 00 00 07 03 00 B9 AB B4 10 00 00 00 3B F2

　　63 36 60 EF 5D EB 06 6F E6 77 03 17 AD 91 04 03

　　00 A9 B5 B2 04 00 00 00 3C A8 93 06

　　我知道在座的懒人很多（包括我自己），我特地在QQPwdFinality.exe文件中加入了一个"产生EWH.DB文件"选项，我知道你可能连这都懒得勾，所以默认情况下，我帮你勾上了。 你可以选择任何口令和循环次数来形成EWH.DB文件，文件会生成在当前的目录下。

好了，现在，你再也不用拿着你那个EWH.DB文件到处奔波了，你就用这个吧，毛爷爷不是说过吗？打击敌人的同时还要保护自己，你用自己的口令到处看别人的记录，查出来多不好，况且，一旦忘记删掉了，被受害者拿去，访高手找名人，那你就可能重新申请QQ号了。不过，如果按照这个原理将自己的QQ改造一下，你就比任何人都更快地进入QQ，抢先零点几秒找到PLMM。但是千万别干坏事哦，如果你将别人的AST改成FFFFFF7F的话，估计他要等一天才能和自己心爱的MM聊天了，你忍心下手吗？是不是有人想到发明一个病毒，专门修改这个号，让登录越来越慢啊呵呵。

　　其实，腾讯稍做努力便可以改掉这个问题，要么在每个QQ Data结构后面加一个Hash验证，要么将用户的QQ号作为密钥，对口令进行加密。最简单的就是用QQ号取代MD5算法中的那个基本字串（即便那几十万个循环中用了一次），这样，自己的EWH.DB就只能自己用了，这才是数字指纹的真正用途嘛。也许你会说，这么做知道了算法还是徒劳，但是，至少可以打破现在的局面——只要会用鼠标的都可以修改EWH.DB，显得这些研究破解的同志多么没有存在的价值啊。

　　以上谈的这些东西总的说起来都是一些雕虫小技，估计有一半的人看到中途就睡着了，坚持下来的请跟随我进入下一个章节，如果最后还有幸存者，我希望和你交个朋友：）

　　谈到这里，我想，这篇文章不太适合高手拜读，如果你是高手并且很无聊地走到这里，那么，你可以休息了，走的时候别忘记关灯关门哦。

　　下面，我们谈谈关于网络的话题。

　　2、QQ网络登录时存在的问题

　　MD5的算法固然不错，但并不能取代传统的算法，那种可逆算法在任何时候都是必要的，特别在网络里。我们可以反证一下，如果你在注册QQ或者修改密码的时候，腾讯公司得到的是MD5 Hash，他怎么能知道你原来的密码是多少呢？他绝对不会和我们一样傻，通过暴力破解的方式得到吧。当然，腾讯公司也可以只要MD5，如果是这样，他就等于失去了一次对用户的隐私进行窥探的机会，这对于任何一个公司来说都是不可能的。

　　退一步说，即使有的公司宣布，为了用户利益，对用户的密码不感兴趣，但是，他还是要知道是谁采用了合法的方式登录，因此，最终都不能免俗，都必须从用户发来的网络包中提取信息来完成身份的校验，以便对上帝们发出邀请或对恶魔们进行拒绝，OK，如果魔鬼扮成上帝呢？

### QQ2009协议分析备忘录

2009-10-30 15:12:37|  分类： [默认分类](http://etian4ever.blog.163.com/blog/#m=0&t=1&c=fks_082071080082087074087082074065083085084070083080083)|字号 订阅

0x0017 (receive message----WAN2LAN): for QQ 2008

0:  44 60 B7 16        //from: QQ number

4:  06 82 B4 04        //to: QQ number

8:  00 05 7A 7D        //sequence number

12: DB 85 31 B5        //from ip

16: 1F 40              //port: 8000

18: 00 09             //IM type

20: 00 00

22: 00 00              //len

---------------------------------------------------------------------

24: 12 21              //version

26: 44 60 B7 16        //from: QQ number

30: 06 82 B4 04        //to: QQ number

34: F1 D5 A9 21 8C 14 A9 54 F7 DE 69 C8 01 A5 47 D6    //16 Bytes

50: 00 0B         //content type: TEXT

---------------------------------------------------------------------

52: 24 26         //session id

54: 4A B0 3C 0A   //time: 2009-09-16 09:14:50

58: 02 0A         //face

60: 00 00 00 01   //??

64: 01            //slice count

65: 00            //slice number

66: 58 00         //message id

68: 01            //auto replay?      01:NO    02:YES

---------------------------------------------------------------------

69: 68 65 6C 6C 6F 20

00 0A 00 00 00 00 86 02 CB CE CC E5 0D    //font etc.

0x00ce(receive message----WAN2LAN): for QQ 2009

0:  44 60 B7 16        //from

4:  06 82 B4 04        //to

8:  00 05 2E D3        //sequence

12: 77 93 0D 16        //from ip

16: 1F 40              //from port

18: 00 A6              //IM type

20: 00 00

22: 00 0D              //len

00 01 00 04 00 00 00 00 00 03 00 01 02

---------------------------------------------------------------

24: 19 0F                  //version

26: 44 60 B7 16            //from

30: 06 82 B4 04            //to

34: FB E4 8C F2 66 F8 7A 23 D0 5E 22 71 1A 1B 50 60    //16 bytes

50: 00 0B                  //contents type

----------------------------------------------------------------

52: 16 7F                       //session id

54: 4A C1 69 34                 //time

58: 02 0A                       //face

60: 00 00 00 01                 //??

64: 01                          //slice count

65: 00                          //slice number

66: 00 00                       //message id??

68: 01                          //auto replay

69: 4D 53 47 00 00 00 00 00          //MSG00000

77: 4A C1 69 35                          //time

81: AE B9 B6 00 00 00 00 00 09 00 86 00 //12 bytes

93: 00 06                                //font name len

E5 AE 8B E4 BD 93                    //font name: 宋体

95: 00 00                            //??

97: 01                                   //contents type, 1–text  2–face  3-image

98: 00 18                                //len

100:     01                                   //is 01 if text or face, 02 if image

101:     00 15                                //message len

103:     E4 B8 AD E5 8D 8E E4 BA BA E6 B0 91 E5 85 B1 E5 92 8C E5 9B BD   //contents：中华人民共和国

======================================================================================

44 60 B7 16

06 82 B4 04

00 0B 7E 8B

77 93 0D 14

1F 40

00 09

00 00

00 00

12 21

44 60 B7 16

06 82 B4 04

74 99 84 F4 8B CD 20 FF FF AD 00 8D 38 58 A7 30

00 0B

33 DD

4A C2 F1 F8

02 0A

00 00 00 01

01

00

CA 00

01

14 42 20

00 0A 00 00 00 00 86 02 CB CE CC E5 0D

================================================================================

44 60 B7 16

06 82 B4 04

00 0D 24 E7

DB 85 31 B5

1F 40

00 09

00 00

00 00

12 21

44 60 B7 16

06 82 B4 04

AF 5B 26 FE 09 38 20 E7 E3 80 D7 85 21 4E 5D 24

00 0B

61 41

4A C0 62 63

02 0A

00 00 00 01

01

00

9C 00

01

B9 FA C7 EC BF EC C0 D6 A3 A1 20

00 0A 00 00 00 00 86 02 CB CE CC E5 0D

06 82 B4 04

44 60 B7 16

00 0A

B9 F4 79 0E 62 A1 1F 40

00 84

19 0F

06 82 B4 04

44 60

B7 16 A5 FF

4A 7B 3A D5 E9 90 BF C9 38 AB 18 86 1C 8A

00 0B

47 01 4A B0 57 5E 02 0A 00 00 00 01 00 00 00 00

00 00 00 00 01 00 00 00

01

BA C3 B0 A1 B0 A1 B0 A1 20

00 09 00 00 FF 00 86 22 CE A2 C8 ED D1 C5 BA DA 11

44 60 B7 16 06 82 B4 04 00 05 51 C9 DB 85 31 B5 1F 40 00 09 00 00 00 00 12 21 44 60 B7 16 06 82

B4 04 F1 D5 A9 21 8C 14 A9 54 F7 DE 69 C8 01 A5 47 D6 00 0B 4E 31 4A B0 48 EA 02 0A 00 00 00 01

01 00 5A 00 01 C4 E3 BA C3 20 00 0A 00 00 00 00 86 02 CB CE CC E5 0D

44 60 B7 16 06 82 B4 04 00 07 A1 CB DB 85 3C 3B 1F 40 00 09 00 00 00 00 12 21 44 60 B7 16 06 82

B4 04 F1 D5 A9 21 8C 14 A9 54 F7 DE 69 C8 01 A5 47 D6 00 0B 4E 07 4A B0 48 DD 02 0A 00 00 00 01

01 00 59 00 01 47 6F 6F 64 20 6D 6F 72 6E 69 6E 67 2E 20 00 0A 00 00 00 00 86 02 CB CE CC E5 0D

44 60 B7 16 06 82 B4 04 00 06 ED E1 DB 85 3C 3B 1F 40 00 09 00 00 00 00 12 21 44 60 B7 16 06 82

B4 04 F1 D5 A9 21 8C 14 A9 54 F7 DE 69 C8 01 A5 47 D6 00 0B 4D D6 4A B0 48 CE 02 0A 00 00 00 01

00 00 00 00 02 C4 FA BA C3 A3 AC CE D2 CF D6 D4 DA D3 D0 CA C2 B2 BB D4 DA A3 AC D2 BB BB E1 B6

F9 D4 D9 BA CD C4 FA C1 AA CF B5 20 00 09 00 00 00 00 86 02 CB CE CC E5 0D

44 60 B7 16 06 82 B4 04 00 06 ED E1 DB 85 3C 3B

44 60 B7 16 06 82 B4 04 A6 CB E0 B8 FF FF FF FF 00 0B 00 79 00 00 00 00 44 60 B7 16 00( writing)

00 00 27 10 06 82 B4 04 00 0D B0 F0 77 93 0D 15 1F 40 00 6B 00 00 00 00 04 00 00 00 00

0x00cd (send message----LAN2WAN)

0:  06 82 B4 04            //from

4:  44 60 B7 16            //to

8:  00 00 00 0D

12: 00 01 00 04

16: 00 00 00 00

20: 00 03 ````````//len?

00 01 01      //???

22: 19 0F

--------------------------------------------------------------

24: 06 82 B4 04

28: 44 60 B7 16

32: 17 8E 55 0C 26 D4 2C 2B 3F A7 BF EE 61 5A D1 CF

48: 00 0B                  //type

50: 32 8E                  //sequence number

52: 4A C1 69 B5            //time

56: 02 0A                  //face

58: 00 00 00 01            //font attribute

62: 01                     //slice count

63: 00                     //slice number

64: 00 00                  //message id

66: 01                     //auto replay

67: 4D 53 47 00 00 00 00 00     //MSG00000

75: 4A C1 69 B5                 //time create

79: 14 9C E5 A7                 //random

83: 00 FF 00 00                 //???

87: 09 00 86 22                 //????

91: 00 0C                       //font len

E5 BE AE E8 BD AF E9 9B 85 E9 BB 91  //font name:utf8

93: 00 00

95: 01

96: 00 10

98: 01

99: 00 0D                        //message len

68 6F 77 20 61 72 65 20 79 6F 75 3F 0D

send to QQ2008

0:   06 82 b4 04                 //from

4:   44 60 b7 16                 //to

8:   00 00 00 08                 //??

12:  00 01 00 04                 //??

16:  00 00 00 00                 //??

20:  19 0f                       //version

22:  06 82 b4 04                 //from

26:  44 60 b7 16                 //to

30:  a8 ec ab 56 18 49 a6 d6 35 0c 26 2e d0 8f f4 f5    //16 bytes

46:  00 0b                      //type

48:  45 45                       //sequence number

50:  4a d4 1a 32                 //time create

54:  02 0a                       //face

56:  00 00 00 01                 //font attribute

60:  01                          //slice count

61:  00                          //slice number

62:  00 00                       //message id

64:  01                          //auto replay?

65:  4d 53 47 00                 //”MSG00000”

69:  00 00 00 00

73:  4a d4 1a 32                 //time create

77:  9a ce a5 b5                 //random number

81:  00 ff 00 00                 //???

85:  09 00 86 22                 //??

89:  00 0c                       //length of font

e5 be ae e8 bd af e9 9b 85 e9 bb 91  //微软雅黑

91:  00 00

93:  01

94:  00 06                       //content\_len+3

96:  01

97:  00 03                       //content\_len

99:  e5 a5 bd

===============================================================================

06 82 B4 04

44 60 B7 16

00 00 00 08

00 01 00 04

00 00 00 00

19 0F              //version

06 82 B4 04

44 60 B7 16

A5 FF 4A 7B 3A D5 E9 90 BF C9 38 AB 18 86 1C 8A

00 0B

41 CC 4A B0 3C 16 02 0A 00 00 00 01 01 00 00 00 01 4D 53 47 00 00 00 00 00 4A B0 3C 16 F8 95 00 69 00 FF 00 00 09 00 86 22 00 0C E5 BE AE E8 BD AF E9 9B 85 E9 BB 91 00 00 01 00 10 01 00 0D 47 6F 6F 64 20 6D 6F 72 6E 69 6E 67 2E

06 82 B4 04 0A 7A DF 61 00 00 00 00 18 37 06 82 B4 04 0A 7A DF 61 D7 0E 7F 7E 05 04 0E EA 08 9C

1D F5 C3 FC 7E A7 00 AF 2C 2D 4A A5 B4 9F 02 0A 00 00 00 01

06 82 B4 04 0A 7A DF 61 00 00 00 08 00 01 00 04 00 00 00 00 18 37 06 82 B4 04 0A 7A DF 61 D7 0E

7F 7E 05 04 0E EA 08 9C 1D F5 C3 FC 7E A7 00 0B 33 87 4A A5 B4 BC 02 0A 00 00 00 01 01 00 00 00

01 4D 53 47 00 00 00 00 00 4A A5 B4 BC 38 63 95 E3 00 FF 00 00 0A 00 86 22 00 0C E5 BE AE E8 BD

AF E9 9B 85 E9 BB 91 00 00 01 00 12 01 00 0F E6 96 B0 E5 AE B6 E5 BE 88 E7 88 BD E5 90 A7

06 82 B4 04 0A 7A DF 61 00 00 00 08 00 01 00 04 00 00 00 00 18 37 06 82 B4 04 0A 7A DF 61 D7 0E

7F 7E 05 04 0E EA 08 9C 1D F5 C3 FC 7E A7 00 0B 33 88 4A A5 B6 10 02 0A 00 00 00 01 01 00 00 00

01 4D 53 47 00 00 00 00 00 4A A5 B6 10 8D D7 47 36 00 FF 00 00 0A 00 86 22 00 0C E5 BE AE E8 BD

AF E9 9B 85 E9 BB 91 00 00 01 00 1B 01 00 18 E4 B8 BB E8 A6 81 E6 98 AF E6 87 92 E5 BE 97 E8 B7

91 E8 BF 87 E5 8E BB

06 82 B4 04 44 60 B7 16 00 00 00 08 00 01 00 04 00 00 00 00 19 0F 06 82 B4 04 44 60 B7 16 A5 FF

4A 7B 3A D5 E9 90 BF C9 38 AB 18 86 1C 8A 00 0B 47 00 4A B0 48 FC 02 0A 00 00 00 01 01 00 00 00

01 4D 53 47 00 00 00 00 00 4A B0 48 FC E7 3A D1 A5 00 FF 00 00 09 00 86 22 00 0C E5 BE AE E8 BD

AF E9 9B 85 E9 BB 91 00 00 01 00 0F 01 00 0C E5 A4 A9 E6 B0 94 E6 99 B4 E6 9C 97

06 82 B4 04 44 60 B7 16 00 00 00 08 00 01 00 04 00 00 00 00 19 0F 06 82 B4 04 44 60 B7 16 A5 FF

4A 7B 3A D5 E9 90 BF C9 38 AB 18 86 1C 8A 00 0B 46 FF 4A B0 48 CD 02 0A 00 00 00 01 01 00 00 00

01 4D 53 47 00 00 00 00 00 4A B0 48 CD 9E D9 CE CA 00 FF 00 00 09 00 86 22 00 0C E5 BE AE E8 BD

AF E9 9B 85 E9 BB 91 00 00 01 00 08 01 00 05 68 65 6C 6C 6F

0x0016(send message----LAN2WAN) QQ2008

44 60 B7 16 06 82 B4 04 12 21 44 60 B7 16 06 82 B4 04 4E 5A 7A B0 E9 54 D0 EB 49 16 79 55 1A 8F C6 48 00 0B 7D 05 4A B0 57 41 02 0A 00 00 00 01 01 00 13 00 01 68 65 6C 6C 6F 20 00 0A 00 00 00 00 86 02 CB CE CC E5 0D

=============================================================================

群相关

0x0002: Qun command

72               //qun info

00                               //result： must be 00

78 8D B5 E9             //interior number

04 BD E2 29             //exterior number

00 00

00

03                               //status

01                               //type

00 01 00 01

06 82 B4 04              //owner

02                               //authority type

00 00 01 8B 00 00

00 00 00 00              //category

00 64                          //max member

01 00 00 00 01 00 00 00 22

08                               //length of name

4F 75 72 20 54 65 61 6D          //name

00

00                               //separator

00                               //length of ann: announce??

00                               //length of introduction

00 38 1D 8B 6B DE 0D 3A 7A 09 B2 17 88 B2 89 F3 23 56 23 7D 09 D2 19 AF E2 E0 8C 2D 8B 98 E6 BD 62 98 DA 2F 46 A3 61 0A FA 8F 6F EA E7 D0 DE CE DD 7B 5C CF 04 7A B4 81 01 F9

06 82 B4 04

00

06 82 B4 04

00 00

--------------------------------------------------------------------------------------------------------------------------

2A                                        //send qun message

78 8D B5 E9                       //interior number

00 3B

00 01                                   //text type

01                                         //slice count

00                                          //slice number

00 00                                   //id

00 00 00 00

4D 53 47 00                       //MSG00

00 00 00 00

4A D0 35 62                       //time create

E6 E2 B1 C5                       //random

00 00 00 00                        //zero

09 00 86 00                        //??

41：         00 06                                   //font name length

E5 AE 8B E4 BD 93                    //font name: 宋体（utf8）

43：         00 00

01

00 0C                                   //length+3

01                                         //??

49：         00 09                                   //length of content

E5 A4 A7 E5 AE B6 E5 A5 BD   //contents

0x0017: 接收群消息

QQ2009

0：  78 8D B5 E9             //interior number

4：  44 60 B7 16              //to

8：  00 09 39 CA              //sequence number

12：77 93 13 C6              //from ip

16：1F 40                          //port

18：00 52                          //type

------------------------------------------------------------------------------------------------

20：00 00 00 00              //QQ2009

24：04 BD E2 29             //exterior number

28：01                               //normal qun or temp qun

29：44 60 B7 16              //from

33：00 00                          //zero

35：01 13                           //message  id

37：4A D0 35 61             //message time

41：00 00 00 23

-----------------------------------------------------------------------------------------------

45：00 3B

47：00 01

49：01

50：00

51：00 00

53：00 00 00 00

57：4D 53 47 00              //MSG00

61：00 00 00 00

65：4A D0 35 62

69：E6 E2 B1 C5

73：00 00 00 00

77：09 00 86 00

81：00 06                          //length of font

E5 AE 8B E4 BD 93

83：00 00

85:   01

86:   00 0C                         //length+3

88:   01

89:   00 09                          length

91:   E5 A4 A7 E5 AE B6 E5 A5 BD   //content

QQ2008

0:      78 8D B5 E9               //interior number

4:      06 82 B4 04               //to:         109229060

8:      00 02 E1 D5              //sequence number???

12:   3A 3C 0F 3D             //from ip

16:   1F 40                          //port

18:   00 2B                         //IM  type

20:   00 00

22:   00 00                          //len

24:   04 BD E2 29               //exterior number

28:   01                               //normal qun or temp qun

29:   44 60 B7 16              //from:     1147189014

33:   00 00                           //zero

35:   01 59                           //message ID

37:   4A D2 EF 28              //message time

41:   00 00 00 23

---------------------------------------------------------------------------------------------

45:   00 28

47:   00 01

49:   01

50:   00

51:   19 A4

53:   00 00 00 00

57:   68 65 6C 6C 6F 2C 20 65 76 65 72 79 6F 6E 65 2E 20               //contents

00 0A 00 00 00 00 86 02 CB CE CC E5 0D                                     //fonts

webQQ

*0x17*

0:   06 82 B4 04

4:   44 60 B7 16

8:   00 01 FE AB

12:  79 0E 62 A1

16:  1F 40

18: 00 09            //im type

20:  00 00

22:  00 06              //len

00 05 00 02 00 29

24:  0E 05              //version?

26:  06 82 B4 04

30:  44 60 B7 16

34:  49 4A 71 50 47 34 7A 48 62 59 71 61 6A 77 61 63

50: 00 0B           //content type

52:  00 18

54:  4A D7 DE 20        //time created

58:  00 00              //face??

60:  2F 7B D5 4C

64:  01

65:  00

66:  00 00              //MESSAGE ID?

68:  01

69:  C4 E3 BA C3 0A A1 BE CC E1 CA BE A3 BA B3 C1 C4 AC D6 AE C9 F9 28 31 30 39 32 32 39 30 36 30 29 D5 FD D4 DA CA B9 D3 C3 57 65 62 51 51 A3 BA 68 74 74 70 3A 2F 2F 77 65 62 2E 71 71 2E 63 6F 6D 2F 3F 77 A1 BF 20

00 09 00 00 00 00 86 02 54 61 68 6F 6D 61 0F

============================================================================================

*0xcd (the same as sending to 2008)*

0:   44 60 B7 16

4;   06 82 B4 04

8:   00 00 00 08

12:  00 01 00 04

16:  00 00 00 00

20:  19 0F

22:  44 60 B7 16

26:  06 82 B4 04

30:  3F FB DA 6C 68 A6 DB 4C 66 24 26 4D 98 E0 7C A4

00 0B

26 FD

4A D7 DE 2D

02 0A

00 00 00 01

01

00

00 00

01

4D 53 47 00 00 00 00 00

4A D7 DE 2D

12 EA 48 A5

00 00 00 00

09 00 86 00

00 06                  //length of font

E5 AE 8B E4 BD 93      //songti

00 00

01

00 0C                  //content\_len+3

01

00 09                  //length of content

64 61 6A 69 61 68 61 6F 20

06 82 B4 04

44 60 B7 16

00 02 9E DC

79 0E 62 A1

1F 40

00 09

00 00

00 06

00 05 00 02 00 29

0E 05

06 82 B4 04

44 60 B7 16

49 4A 71 50 47 34 7A 48 62 59 71 61 6A 77 61 63

00 0B

00 1F

4A D7 DE 39

00 00

2F 7B D5 4C

01

00

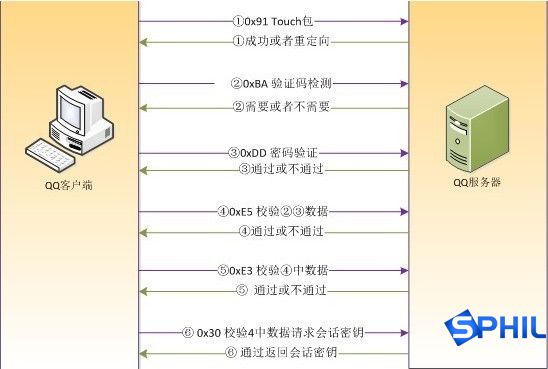
00 00

01

BA C7 BA C7 20

00 09 00 00 00 00 86 02 54 61 68 6F 6D 61 0F

# QQ2011协议分析[原创] 2011-04-07 11:17:06   来源：思派尔科技：吕腾飞   评论：[0](http://www.sphil.com/html/2011/Wikipedia_0407/194.html#comment_iframe) 点击：3850



上图为QQ登录描述

[NO.1 2011-04-02 09:26:45 093 SEND]

02 21 07 00 91 29 83

0B C8 FB 29 02 00 00 00 01

01 01 00 00 64 53

8A 0F 53 42 B1 61 4A D3 D9 94 F0 64 DB AD 83 4C //tea key

F4 79 86 3A BC 01 07 86 B0 C3//密文start

60 8D F3 F3 46 D5 5B 59 B6 AA B0 47 9C CD 2E EE

00 BA 41 90 B6 40 ED B2 96 E1 75 3F EF 6F 9D 4C

BE E1 EF 2E 79 B7 //密文end

//解密结果

【

00 01 00 00 08 04 01 E0 00 00 03 50 00 00 00 01

00 00 0C EB 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00

】

03

[

02 //包头

21 07 //版本号

00 91 //命令

29 83 //包序号

0B C8 FB 29 //QQ号码:197720873

02 00 00 00 01 01 01 00 00 64 53 //固定，QQ版本号不同则不同

8A 0F 53 42 B1 61 4A D3 D9 94 F0 64 DB AD 83 4C //0x91密钥

//密文解密----------------------------------------------------

00 01 //固定两字节

00 00 08 04 01 E0 //0091Data01（在后面的命令里面要用到的）

00 00 03 50 00 00 00 01 00 00 0C EB //0091Data02（在后面的命令里面要用到的）

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 //首次发送为15字节0

//end密文解密-------------------------------------------------

03 //包尾

]

[NO.2 2011-04-02 09:26:45 116 RECEIVE]

02

21 07

00 91

29 83

0B C8 FB 29 [QQ号码：197720873]

00 00 00

//密文------解密方式用发送包中的密钥解密

61 7B D5 EF 7B 47 D2 BA 01 A5 7B 32 AC CB 50 F0

7C 13

6C AB D5 59 81 A2 88 AB A2 D9 2B E1 B4 23 E1 5F

36 58 FE 0E 37 66 B8 B3 7F 1C F9 FD FF 62 B1 BF

41 E4 58 58 87 03 F4 D6 4E D3 4C 5B 9D 2B BA 8F

BE 9A 09 46 DE 37 F3 8F B6 AF 26 58 05 E4 4B 33

0B 7F 71 C2 7B BC

//解密结果---------------------------

【

00 4D 96 7B 44 6F AD 4F D6 00 00 00 00 00 00 00

00 00 38 21 B6 66 0A 70 9C 2E 6F C4 96 06 24 24

ED 89 4E B1 F8 7A D5 92 35 5A D2 CF 91 22 EB E0

A3 5F 71 DB C8 8F 7B 61 0C 59 C1 E4 D8 62 86 3A

1A 82 CF 6D 40 2E 57 84 FF 89 B8 00

】

03

[

02 //包头

21 07 //版本号

00 91 //命令

29 83 //包序号

0B C8 FB 29 //QQ号码:197720873

00 00 00 //固定全为0

//密文-------------------------------------------------------

00 //接触成功

4D 96 7B 44 //登录时间:2011/4/2 9:26:28

6F AD 4F D6 //登录IP地址:111.173.79.214

00 00 00 00 00 00 00 00 //固定8字节0

00 38 //0091\_Token长度：56字节

21 B6 66 0A 70 9C 2E 6F C4 96 06 24 24 ED 89 4E

B1 F8 7A D5 92 35 5A D2 CF 91 22 EB E0 A3 5F 71

DB C8 8F 7B 61 0C 59 C1 E4 D8 62 86 3A 1A 82 CF

6D 40 2E 57 84 FF 89 B8

00 //接触成功

// end密文-----------------------------------------------------------

03 //包尾

]

[NO.3 2011-04-02 09:26:45 117 SEND]

02

21 07 //版本号

00 BA //命令

40 5C

0B C8 FB 29//[QQ号码：197720873]

02 00 00 00 01 01 01 00 00 64 53 //根据版本固定

DA CE 38 95 60 4D C6 0D D5 92 4F AB 8F E7 03 AF //teakey

5E 80 CB 67 AE A7 B4 BE A4 5D

D2 B5 A8 4E 5B A8 AB 9D 53 DB E1 B9 E3 93 97 6B

25 A2 E3 BE 52 C3 38 F1 D4 FF FD A8 1E 76 10 C1

85 4A 5A C2 5F F2 F9 A5 B5 AF 51 F0 29 13 8B CD

ED 88 D1 D7 82 A2 33 29 31 A0 0A 04 69 FE F1 4F

A3 70 F3 23 A5 F4 52 58 68 42 DE 6B 45 7F A3 CE

3E 92 A2 0C 06 B1 08 11 52 D9 2C A5 4A AC

//解密后结果-------------------------------------

【

00 01 00 00 08 04 01 E0 00 00 03 50 00 00 00 01

00 00 0C EB 00 38 21 B6 66 0A 70 9C 2E 6F C4 96

06 24 24 ED 89 4E B1 F8 7A D5 92 35 5A D2 CF 91

22 EB E0 A3 5F 71 DB C8 8F 7B 61 0C 59 C1 E4 D8

62 86 3A 1A 82 CF 6D 40 2E 57 84 FF 89 B8 03 00

05 00 00 00 00 00 00 00

】

//end----------------------------------------------

03

[

02 //包头

21 07 //版本号

00 BA //命令

40 5C //包序号

0B C8 FB 29 //QQ号码:197720873

02 00 00 00 01 01 01 00 00 64 53 //固定，QQ版本号不同则不同

DA CE 38 95 60 4D C6 0D D5 92 4F AB 8F E7 03 AF //0xBA密钥

//解密后明文--------------------------------------------------------

00 01 //固定两字节

00 00 08 04 01 E0 //0091Data01

00 00 03 50 00 00 00 01 00 00 0C EB //0091Data02

00 38 //0091\_Token长度：56字节

21 B6 66 0A 70 9C 2E 6F C4 96 06 24 24 ED 89 4E

B1 F8 7A D5 92 35 5A D2 CF 91 22 EB E0 A3 5F 71

DB C8 8F 7B 61 0C 59 C1 E4 D8 62 86 3A 1A 82 CF

6D 40 2E 57 84 FF 89 B8

03 00 05 00 00 00 00 00 00 00 //固定

//end解密后明文---------------------------------------

03 //包尾

]

[NO.4 2011-04-02 09:26:45 200 RECEIVE]

02 //title

21 07 //版本号

00 BA //命令

40 5C //命令序列号

0B C8 FB 29//[QQ号码：197720873]

00 00 00 //好像是固定的来标识密文的开始吧

6E 7F 39 06 DF 42 B3 24 BE 27 BA FF 23 5F DD 9E 03 8F

42 2A BE E8 3B E8 A0 31 E7 9E 24 F1 FC 72 31 B6

C2 29 C7 FD CE 0C F9 61 CA 63 06 FD C3 54 C2 96

FF F3 C8 27 E3 5B 97 6D 81 5A 67 85 8B E3 EC 16

77 87 93 C8 E7 74 EA 0C C1 23 DA 90 3E 20

//解密后明文----------------------------------------------

【

03 00 05 00 00 00 00 00 00 38 6F 93 B7 CE 6E 78

57 23 76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43

A8 4F D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB

50 54 1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1

70 71

】

//end解密后明文-------------------------------------------------

03

[

02 //包头

21 07 //版本号

00 BA //命令

40 5C //包序号

0B C8 FB 29 //QQ号码:197720873

00 00 00 //固定

//解密后明文-------------------------------------------------

03 //验证结果：03表示成功，04表示需要验证码

00 05 //固定

00 //是否需要验证码：0不需要，1需要

00 00 00 00 //验证码，需要验证码时为00 00 01 23，不需要时为全0

00 38 //00BA\_Token长度：56字节

6F 93 B7 CE 6E 78 57 23 76 18 E7 D8 DC 7A 67 C8

FF 65 5A 2F 18 43 A8 4F D2 A6 09 09 94 21 58 EF

E8 7A 44 B8 3A CB 50 54 1B FF CD 00 A6 86 CB E8

28 5C 45 BC 06 D1 70 71

//end解密后明文---------------------------------------------

03 //包尾

]

[NO.5 2011-04-02 09:26:45 204 SEND]

02 //title

21 07 //版本号

00 DD //命令

72 33 //命令序列号

0B C8 FB 29//[QQ号码：197720873]

02 00 00 00 01 01 01 00 00 64 53 //根据QQ版本固定

B9 EC 62 84 80 97 A2 3F 1A A4 25 F9 6A 7D 7B 8A //teakey

//密文

5A C9 3A E6 2E C1 F7 64 39 CC

72 95 06 B1 57 66 DF 3A 5F 95 F3 9E F8 B0 C1 D3

16 61 58 A1 CE C4 01 D2 BF 23 CF F6 EC 8A AA 30

53 90 6E 45 48 D5 0A 99 26 1A 61 7E 4B A3 60 57

C3 D2 4D 66 AB 44 EB A5 58 A8 9C 49 4F ED 3D D0

88 75 93 CF 3D F9 9E 4A 73 8A 34 5D 75 44 D6 79

7F 9D 26 7D 0F 80 F6 5E 29 2B 3C 2E 88 50 A2 E7

28 EE 97 97 E2 42 20 0F 4B 8E 11 6A 43 3B D4 D0

24 61 6D B2 92 4C 3B 6D F1 47 29 6D 2D E0 38 96

25 72 00 4D 0C BD 47 85 04 A5 5C 55 8F 0D 5E 01

85 72 5E AE A2 F3 0E F3 93 FC C1 B1 55 A1 10 6D

37 07 CD BA D0 1E BC 46 22 A7 A3 21 6C F1 69 BA

AB 20 A0 52 2A EA EA 02 D7 22 0A 92 75 27 6E 65

87 A5 9C D3 0E FE 42 A7 B4 68 03 7D 32 0C A2 BB

2A F3 E2 12 4B 27 0E 05 EC DB AA 28 92 88 93 44

A6 84 2D 40 CB F8 70 9E 02 67 93 03 39 27 A3 B4

89 68 76 F8 8C 57 4D C3 66 8E B7 C8 5C 4C A3 45

61 4A 5E E5 17 5D B4 48 AC F1 30 21 B2 5F 91 84

71 BD D2 52 5E 30 9D 42 81 4B 4E 06 D9 A2 F4 D2

03 A8 A9 A0 17 B3 A5 46 D6 07 86 81 F9 01 8E 9C

14 EA 29 14 92 4D 9B 9F DA 74 80 8E 55 0B EE B9

E3 1F 70 4B A6 AE 28 34 8A B2 E9 89 F0 A0 6F 8E

1F 13 55 19 CD 15 11 9E 4C C2 E2 38 DD 97 41 C1

DF 93 9B C4 B9 58 72 30 39 C2 BE 9C 15 8A DC C2

AF 44 09 0F 13 6B 4A 4B 0A B4 09 A0 85 95 BE D7

58 5E F3 C8 8E E1 DA 74 2E 1D FA E8 7A E7 9D 41

CB 83 6D 79 A1 AF 01 75 DC 20 FF 53 1C 4F D8 01

7B 92 22 3C 6B 4D 91 CA 1F 11 7D B4 EA 05 A3 BC

A4 0C C4 9F E4 8E CA 5A 57 D0 8B C0 B1 34 A1 83

1F E7 AE EF A5 2B C8 D3 AD CE C1 F5 B8 07 FE 40

8E 85 67 FF 9D E4 C8 9D 8D FB B8 E5 91 96 52 EB

6C ED 48 C6 AE 72 84 32 5C F1 A5 5F 0C 08 B8 1C

18 C3 69 F7 75 0F 0F 66 AE DE 2C CB 03 75 29 16

88 41 CA 87 48 CA 0D 93 EF 8A FE 7E 93 7A 09 A0

BA 99 7C BF BC 8E BE B1 11 7A 1A 67 4D D3 9C AC

F3 EB 64 9C 15 4E C3 A2 03 E5 9C 6E 13 BF 3E 92

BC 6F AB 44 72 A5 3E 75 B6 EE 8C 5E A3 14 95 38

36 3C E4 70 4B 9B BB BC 82 1A E6 69 7F 23 11 EA

AC 1F 03 F8 54 D1 3B 4F 0F 08 79 66 76 EB //end密文

//解密结果---------------------------------------------

00 DE 00 01 00 00 08 04 01 E0 00 00 03 50 00 00

00 01 00 00 0C EB 00 38 6F 93 B7 CE 6E 78 57 23

76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43 A8 4F

D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB 50 54

1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1 70 71

00 78 A0 2B FD E9 17 F3 7E 1B 7E 8D 39 5E FD 8A

62 3E 46 90 B0 E5 AA B1 62 CC 15 15 D3 25 6F C4

8E 50 8E 4A 57 03 F9 E7 C5 B2 38 70 53 77 44 98

38 94 9A 71 1C BA 8E E8 85 8F 33 8E F4 A6 25 22

A8 0F C3 54 90 1F 7C 2B 21 D5 83 9C E1 86 CF A5

38 86 9E 35 94 EC 06 29 34 F6 0C 8A A5 2B 1F 8B

5A 8A E1 05 B7 58 6C FA 25 11 FB C6 B9 20 56 A8

13 79 C8 E3 DD 13 EC 9A DC 95 00 14 EB F5 28 BB

2D 0B 0B 1F 2B E9 54 8C 3B 7A B2 29 B1 E2 61 03

01 77 2E 01 CA 18 88 64 00 10 10 B9 D4 75 E5 F1

12 11 F8 53 04 7C 5C C9 95 66 02 16 37 69 27 00

10 76 58 5D 0D D0 A7 21 89 0A 65 CB F4 3B B4 65

8F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00

//end解密结果-----------------------------------------

03

//////////////////////////////////////整理

[

02 //title

21 07 //版本号

00 DD //命令

72 33 //命令序列号

0B C8 FB 29//[QQ号码：197720873]

02 00 00 00 01 01 01 00 00 64 53 //根据QQ版本固定

B9 EC 62 84 80 97 A2 3F 1A A4 25 F9 6A 7D 7B 8A //tea key

00 DE 00 01

00 00 08 04 01 E0 //0x91data1

00 00 03 50 00 00 00 01 00 00 0C EB //0x91data2

00 38 //token长度在e3 e5包中用到

6F 93 B7 CE 6E 78 57 23

76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43 A8 4F

D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB 50 54

1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1 70 71

00 78 //qq密码验证密文长度

A0 2B FD E9 17 F3 7E 1B 7E 8D 39 5E FD 8A

62 3E 46 90 B0 E5 AA B1 62 CC 15 15 D3 25 6F C4

8E 50 8E 4A 57 03 F9 E7 C5 B2 38 70 53 77 44 98

38 94 9A 71 1C BA 8E E8 85 8F 33 8E F4 A6 25 22

A8 0F C3 54 90 1F 7C 2B 21 D5 83 9C E1 86 CF A5

38 86 9E 35 94 EC 06 29 34 F6 0C 8A A5 2B 1F 8B

5A 8A E1 05 B7 58 6C FA 25 11 FB C6 B9 20 56 A8

13 79 C8 E3 DD 13 EC 9A DC 95

/////////////////QQ密码验证密文继续解密------------teakey= md5(md5(密码)+0000（四个字接0）+QQ号码)

【

35 3C E2 73

00 01

0B C8 FB 29 //QQ号码[QQ号码：197720873]

00 00 03 50 00 00 00 01 00 00 0C EB

00 00 00 //固定

BC 30 9A 83 F7 4A 98 C5 8B A7 80 F9 08 FD 41 3A //QQ密码（一次md5）//密码已经完全暴露了呵呵。

4D 96 7B 44 //[ 时间：2011/4/2 9:26:28] 登录时间

00 00 00 00 00 00 00 00 00 00 00 00 00 //固定13个字节0

6F AD 4F D6 //外网 IP地址：111.173.79.214

00 00 00 00 00 00 00 00

00 10//8个字节0

90 70 AC 18 20 D5 D4 44 9C 86 58 7B 57 82 C6 19 //根据版本固定

25 0C D5 AB 84 18 6D EB EC AA 9F E2 A1 01 79 F8  //teakey for  dd  RECEIVE packet

】

00 14 //二十位数据key+crc32 前面为key后面crc32

EB F5 28 BB 2D 0B 0B 1F 2B E9 54 8C 3B 7A B2 29

B1 E2 61 03

01 77 2E //固定

01

CA 18 88 64 //同下

00 10 //同下

10 B9 D4 75 E5 F1 12 11 F8 53 04 7C 5C C9 95 66 //同下

02

16 37 69 27//key的反crc32

00 10 //key长度

76 58 5D 0D D0 A7 21 89 0A 65 CB F4 3B B4 65 8F //16key

-----------------328个0--------------------------

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00

]

[NO.6 2011-04-02 09:26:45 327 RECEIVE]

02 //头

64 53 //版本号

00 DD //命令

72 33 //命令序列号

0B C8 FB 29 //[QQ号码：197720873]

00 00 00 //固定

//加密密文-------------------------------------

5F A6

F2 6C 37 08 24 62 D5 40 59 2F AA C9 EA 90 D7 E6

11 BF D5 79 08 6E A8 24 60 9A A5 5C DA 49 D3 68

E8 8F BC 56 37 3C E9 70 DC 47 A5 D1 AA 0C DA 85

E9 CC 0F 32 F5 03 9D 35 4F C6 F1 94 BA 09 29 DE

91 46 C5 67 F0 3D 7B 8F F3 57 1E C8 56 EA 49 05

FF 78 71 ED 94 B6 49 AF F4 80 A9 C7 F2 A7 81 A1

46 D0 0F 42 6C 59 63 4B 97 C9 54 7B 76 1B 08 DB

C2 EF 72 73 78 A2 A4 58 40 31 26 7F 20 AA A4 3E

44 CD CA 9E 4C CB EC 7E CB E8 B4 DA C5 1B 7C E5

C1 BE C3 07 DB F6 28 29 C7 C8 82 B4 6A 2C 80 66

17 7A 25 69 A2 F8 74 DE 38 AD 69 A2 5E 1A E0 C2

DC FA 3F 7A 31 E4 D2 C3 ED D0 46 39 60 17 0A 9C

FD E9 FA 41 49 47 30 A0 76 87 B6 AB 2F 03 98 8B

5C 5C C7 94 03 3B E5 83 14 91 61 31 21 46 95 D8

F1 73 16 DF 37 9B F9 69 11 6F C3 E9 64 84 82 FB

89 23 C7 3A C3 F2 85 FE D2 DE D5 87 AC EE 6D 6B

81 55 F2 28 DB A8 62 F3 41 47 E1 1A 9D 22 C6 8B

6F F6 DC 98 92 39 80 FA 55 D7 B2 A9 08 E5 70 A6

04 E6 1D C6 0D 90

//end加密密文-----------------------------------------

--解密后明文-------------------------------------------

【

01 19 00 00 20 14 E9 7A 62 E3 FE FF 25 95 2E 93

E7 80 C0 00 AF 29 D5 AE 65 1F 74 A3 75 DB 6C EC

4C 20 64 48 B8 00 98 00 02 4D 96 7B 44 00 90 71

D9 43 A5 4C 10 2C A9 33 A7 7D F6 8C 6D 71 23 22

40 79 27 90 85 D5 30 1E 3C C7 8F 90 B1 02 C9 AB

D3 C1 19 1F 9F C4 C8 30 41 D7 45 FD 54 F1 BE E0

A5 36 BE F9 23 0F 04 02 30 8D 4F EA 3F 56 4E 6D

DF 8F EE 35 94 06 1A 7A D3 28 FB 70 AD 04 4B 83

38 0B 8E 9C 20 E1 F3 C2 EE 74 1F 39 69 7B 13 4B

1D 0F D2 F0 04 7A 73 FF B2 57 BE 4E DA 7E 61 6D

12 C6 5F C0 7C A6 0F 6B 7C 0B 48 DE EF 56 78 60

B8 3A 49 5A B3 4C 5B 54 B9 6F A2 61 79 7C 28 00

38 23 C2 99 DA 27 32 FA 89 3C 85 CC C7 C0 40 50

6B 2F B9 7F B5 1A 5D AC D9 0A 5B FD 70 4B 67 1F

7A 96 47 7E 2D 20 56 84 29 03 EA B7 35 A3 01 ED

8F 65 93 D5 A0 6D F4 B6 72 6A 70 36 4B 34 35 58

4B 61 52 54 69 76 79 37 6D 00 00 43 46 76 72 33

56 41 59 51 59 55 4E 48 4D 79 61 00 00 //285个字符

】

--end解密后明文---------------------------------------

03

///////////////整理////////////////////////////

[

02 //头

64 53 //版本号

00 DD //命令

72 33 //命令序列号

0B C8 FB 29 //[QQ号码：197720873]

00 00 00 //固定

01 19

00 //成功（00验证通过，33或51拒绝登录、BF没有该号码、34密码错误）

00 20 //token0\_auth 长度（32bytes)

14 E9 7A 62 E3 FE FF 25 95 2E 93 E7 80 C0 00 AF

29 D5 AE 65 1F 74 A3 75 DB 6C EC 4C 20 64 48 B8 //token0\_auth

00 98 //时间+token1\_auth 长度

00 02 //固定

4D 96 7B 44 [ 时间：2011/4/2 9:26:28]

00 90 //token1\_auth长度

71

D9 43 A5 4C 10 2C A9 33 A7 7D F6 8C 6D 71 23 22

40 79 27 90 85 D5 30 1E 3C C7 8F 90 B1 02 C9 AB

D3 C1 19 1F 9F C4 C8 30 41 D7 45 FD 54 F1 BE E0

A5 36 BE F9 23 0F 04 02 30 8D 4F EA 3F 56 4E 6D

DF 8F EE 35 94 06 1A 7A D3 28 FB 70 AD 04 4B 83

38 0B 8E 9C 20 E1 F3 C2 EE 74 1F 39 69 7B 13 4B

1D 0F D2 F0 04 7A 73 FF B2 57 BE 4E DA 7E 61 6D

12 C6 5F C0 7C A6 0F 6B 7C 0B 48 DE EF 56 78 60

B8 3A 49 5A B3 4C 5B 54 B9 6F A2 61 79 7C 28 //token1\_auth

00 38 //token2\_auth 长度

23 C2 99 DA 27 32 FA 89 3C 85 CC C7 C0 40 50

6B 2F B9 7F B5 1A 5D AC D9 0A 5B FD 70 4B 67 1F

7A 96 47 7E 2D 20 56 84 29 03 EA B7 35 A3 01 ED

8F 65 93 D5 A0 6D F4 B6 72 //token2\_auth

6A 70 36 4B 34 35 58 4B 61 52 54 69 76 79 37 6D key2\_auth 用在e5 、03请求包里

00 00 //固定

43 46 76 72 33 56 41 59 51 59 55 4E 48 4D 79 61 key3\_auth 用在e5的接收包

00 00 //固定

]

[NO.7 2011-04-02 09:26:45 328 SEND]

02 //包头

21 07 //版本号

00 E5 //命令

03 E9 //命令序列号

0B C8 FB 29 //[QQ号码：197720873]

02 00 00 00 01 01 01 00 00 64 53 //根据版本固定

00 38 //token2\_auth 长度

23 C2 99 DA 27 32 FA 89

3C 85 CC C7 C0 40 50 6B 2F B9 7F B5 1A 5D AC D9

0A 5B FD 70 4B 67 1F 7A 96 47 7E 2D 20 56 84 29

03 EA B7 35 A3 01 ED 8F 65 93 D5 A0 6D F4 B6 72//token2\_auth

//密文-----------------------------------------------------

10 41 16 70 4A 0E AA 62 5D 20 44 9E 54 F0 9D 62

C2 65 C6 7F 84 47 C4 A2 D7 C2 AE 83 CE 39 D6 F2

F8 BC 69 26 C3 26 1E 56 0E F4 3D 0D 83 80 C6 21

65 C0 C0 5A C1 6B 16 40 79 0B DA B3 DE D5 7D D8

36 00 B1 05 83 28 9D 24 25 0F F3 D4 BB 85 3A A5

A5 07 93 50 03 A9 F8 16 DE 78 8F 03 26 3A FA 9A

5D 84 B5 69 7D DC D6 A7 19 F8 2E 08 12 95 6B 04

87 5E 82 FE E8 B5 EF 60 F9 7F E3 46 1F B9 03 D7

ED 74 2C CD D1 C5 7D CC B3 69 F7 A0 83 44 26 CC

53 5E D3 0A A9 20 F7 AD DF D9 C2 7F 5E 93 99 BA

73 FD 9D 1C 57 12 62 0F 38 F3 EC 3C 32 5F FF 89

38 B5 F1 CB E2 D5 33 1C 80 AF A4 52 95 CC CF 0E

F5 D0 E6 28 8A DF 0B 30 D5 79 4A FD 24 06 81 DC

75 D3 4D E7 5E 8D DA 2B 6E 8A 77 CA 3E 3B 9C 1E

C4 AB 29 50 98 EB 5A A6 5B FA 91 65 74 C9 94 6F

87 9C 41 0C F2 FF AD 4D C2 6B D9 D2 BD C9 E1 4E

B2 92 FB 18 EE 93 BE 6D FB DB 6B D0 A6 30 DD C3

35 62 BE 0B 48 A0 13 8B EC B4 AC 59 FE 71 52 4A

[解密结果]-----------------------------------------

01 0E 00 01 01 00 00 08 04 01 E0 00 00 03 50 00

00 00 01 00 00 0C EB 00 38 6F 93 B7 CE 6E 78 57

23 76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43 A8

4F D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB 50

54 1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1 70

71 00 20 14 E9 7A 62 E3 FE FF 25 95 2E 93 E7 80

C0 00 AF 29 D5 AE 65 1F 74 A3 75 DB 6C EC 4C 20

64 48 B8 00 98 00 02 4D 96 7B 44 00 90 71 D9 43

A5 4C 10 2C A9 33 A7 7D F6 8C 6D 71 23 22 40 79

27 90 85 D5 30 1E 3C C7 8F 90 B1 02 C9 AB D3 C1

19 1F 9F C4 C8 30 41 D7 45 FD 54 F1 BE E0 A5 36

BE F9 23 0F 04 02 30 8D 4F EA 3F 56 4E 6D DF 8F

EE 35 94 06 1A 7A D3 28 FB 70 AD 04 4B 83 38 0B

8E 9C 20 E1 F3 C2 EE 74 1F 39 69 7B 13 4B 1D 0F

D2 F0 04 7A 73 FF B2 57 BE 4E DA 7E 61 6D 12 C6

5F C0 7C A6 0F 6B 7C 0B 48 DE EF 56 78 60 B8 3A

49 5A B3 4C 5B 54 B9 6F A2 61 79 7C 28 00 00 01

00 00 00 00

-//end解密明文-------------------------------------

//end--------------------------------------------

03

////////////////整理//////////////////////////////

[

01 0E 00 01 01 //固定

00 00 08 04 01 E0 //0x91data1

00 00 03 50 00 00 00 01 00 00 0C EB //0x91 data2

00 38 //token\_captcha 长度

6F 93 B7 CE 6E 78 57

23 76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43 A8

4F D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB 50

54 1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1 70

71//token\_captcha

00 20 //token0\_auth 长度

14 E9 7A 62 E3 FE FF 25 95 2E 93 E7 80 C0 00 AF

29 D5 AE 65 1F 74 A3 75 DB 6C EC 4C 20 64 48 B8 //token0\_auth

00 98 //时间加token1\_auth 长度

00 02 //固定

4D 96 7B 44   //回应包时间[ 时间：2011/4/2 9:26:28]

00 90 //token1\_auth长度

71 D9 43

A5 4C 10 2C A9 33 A7 7D F6 8C 6D 71 23 22 40 79

27 90 85 D5 30 1E 3C C7 8F 90 B1 02 C9 AB D3 C1

19 1F 9F C4 C8 30 41 D7 45 FD 54 F1 BE E0 A5 36

BE F9 23 0F 04 02 30 8D 4F EA 3F 56 4E 6D DF 8F

EE 35 94 06 1A 7A D3 28 FB 70 AD 04 4B 83 38 0B

8E 9C 20 E1 F3 C2 EE 74 1F 39 69 7B 13 4B 1D 0F

D2 F0 04 7A 73 FF B2 57 BE 4E DA 7E 61 6D 12 C6

5F C0 7C A6 0F 6B 7C 0B 48 DE EF 56 78 60 B8 3A

49 5A B3 4C 5B 54 B9 6F A2 61 79 7C 28 //token1\_auth

00 00 01 00 00 00 00//固定

]

[NO.8 2011-04-02 09:26:45 354 RECEIVE]

02

21 07

00 E5

03 E9

0B C8 FB 29

00 00 00

/////////////////密文/////////////////

63 74

1F 4F EF 4A 9D DB 34 30 E0 DA B6 60 00 63 3F 87

E3 D5 DA A5 FE 98 45 39 AF 00 3B C4 33 E3 61 74

B9 2E 7F A2 A2 B4 91 FB C6 81 68 E2 F0 27 87 C1

10 14 B7 C6 6B E6 38 BA 5E 1F F6 E3 6B D2 F1 C5

7E 8B 0F BC 6A 11 5B 72 17 12 19 AA 89 5E 02 1A

E9 27 B1 8E F1 22 03 58 FB 07 44 05 0B CA AA 77

27 BD F0 3D 1C C9 05 8F C0 49 48 26 33 A2 93 61

5A 59 C6 7C A9 1A 72 74 77 64 D7 3A 32 0F 40 25

9F FA F6 8C 59 BB 8C 40 F6 42 E6 F3 66 44 79 26

9C C6 FF 9B CA A6 67 B2 96 9A 48 F5 5F E8 F3 97

E9 83 43 51 D6 FC 34 07 77 A8 D5 38 BB 84 03 57

68 06 B8 4D 2C 7F 2C C8 F4 93 7A 1C 36 92 78 7B

68 17 E7 F0 0F 5E F3 B4 87 81 60 78 D0 34 D3 EA

1D 79 6B 27 0F 8B BF 46 B1 58 7B C9 D4 06 8B 48

7C C4 F5 EB A7 E1 E4 BA 63 62 6F AD FF 71 C6 69

EA 90 67 A9 92 4D 80 65 06 E3 62 65 15 C1 7C C0

DA E1 8C C2 AB 46 C3 93 77 EB 28 D3 CE CD 6A BB

32 A3 D6 0D 8D A5 34 2B 88 D0 FB 34 00 D4 DF 20

4F 38 01 66 3C FE D4 6E AF E7 8E DA AB 67 60 9E

8D 6C 7D 80 37 19 AC 5B E4 D5 94 1D ED C9 76 79

07 C6 83 01 85 C9 D7 31 3C 1A 49 E4 48 BA 51 D6

D9 01 01 B3 13 9D 4C 8F 2B 12 33 AD 0C 9B 19 53

1B 78 E3 4D 16 6C F1 A6 3A 07 CC CD B3 F5 31 73

4A 69 15 2D 47 5D 9A E3 97 B8 7A ED 47 C3 36 8F

F3 1C E0 86 E1 32 22 E1 D2 FA 3A 42 4E B8 D4 AE

8A 51 E1 94 B0 51 A0 42 A4 F7 4F FB 00 59 30 85

92 DF 9C 3D 73 83 00 F2 1D 70 34 70 24 8A 63 43

3E ED 47 53 35 A7 1E CB C5 F2 5B 5F BC 45 ED 72

F6 8B FA 83 70 AC ED 87 E9 85 7A 48 A5 25 75 D0

CC 5D 4D BC 1B B8 3C C3 2F 75 69 F0 14 46 1A 0B

62 7B 0D 15 36 A4 88 43 74 CE 27 6D 87 1E C3 26

E4 F1 73 BC C8 C1 24 65 73 B7 D3 7A 74 98 D3 00

F9 AD DA E6 43 EE 83 DF D8 DA 33 03 F9 6F 3B 03

78 73 11 08 4F 28 1A A3 DD FF 53 73 95 14

////////end密文////////////////////////////////////////

///解密结果//////////////////////////////////////////////

[

02 0D 01 00 4A 79 38 4E 75 70 45 37 44 52 61 73

62 61 6A 49 00 00 00 01 00 00 00 64 00 E4 00 03

4D 96 7B 44 6F AD 4F D6 00 00 00 00 00 00 00 00

00 D0 2F 48 4C 8A C9 35 76 E3 70 1F 0D 20 81 28

B6 4C 12 84 2C DE 3B A9 8A 9D 3B 8F 18 A7 F5 BC

26 10 9F 4F A5 8C AC 79 08 3F 92 F0 34 AE A4 76

51 A9 D7 73 63 24 C5 BB B3 0B 52 F9 04 61 39 49

67 99 46 76 37 65 52 E6 3D 2B 29 26 D3 40 91 E1

4C 59 DD 70 B1 73 60 24 10 54 3E 11 79 E7 35 5A

5A EA E0 B6 7A EC 04 BE 9F 4E B8 AD 22 FF 01 DB

E0 AD B2 34 1F 90 B1 53 96 19 13 FD C3 C1 78 10

B6 CE 68 87 CD BC 0C 2C AC BD 75 5B D4 5A 69 86

7F B0 1A 53 AC CC 35 48 8C 3E 46 1D 21 6A F9 26

AD 4A 0D 4F A9 56 15 3D 46 34 9C 4C EB B0 EF 38

EE C7 74 63 75 7A 66 1C CF F8 E4 6E 53 0E 00 12

62 7E 03 07 38 D2 50 0B 57 83 A6 B3 31 36 2F E3

27 61 4A 62 52 4E 6B 47 4D 7A 32 32 36 79 36 4E

51 6E 00 78 00 01 4D 96 7B 44 00 70 F4 98 63 A4

54 BD FB 73 21 A0 6A 78 FA 34 50 B4 4D 56 A1 AF

EE 35 99 D7 BD 53 0F 0D B7 06 2B 58 E6 C9 74 E6

30 FB 3E C8 BF E6 BE 34 35 11 7B 02 CE 3D 20 5F

03 B1 32 F9 9B 67 4C CF 89 00 FE 30 81 1C BE 72

E4 3F F3 BF 6C 59 E1 35 2A C1 BC 14 B6 C6 E6 E0

D3 88 6A CA 36 49 67 4F E8 DF 7B F3 8C 06 A9 4D

8B A6 73 0E EA C7 F5 29 0D E0 63 3A 00 00 0E 02

00 01 51 80 00 00 00 3C 00 02 00 73 01 4E 43 52

46 4E 73 58 62 56 65 6E 4D 58 65 49 4D 00 60 00

01 4D 96 7B 44 00 58 E7 89 52 4B 12 AC 30 66 D7

D4 1F A1 7F 6C 86 C7 04 35 99 4B 03 D5 87 2D F4

C5 8E 76 EA 6A 15 13 26 6B 83 06 51 73 53 8D FD

04 1B 2E 9E FC 41 BE D5 E7 27 67 69 61 24 4F 91

08 23 90 90 A5 41 B8 03 79 35 7A 86 C2 02 5A 37

A8 6C E3 9D 58 AB 74 F7 A9 38 4F DC 68 05 C0 00

00

]

03

//////////////////整理/////////////////////////

[

02 //包头

21 07 //版本号

00 E5 //命令

03 E9 //命令序列号

0B C8 FB 29//[QQ号码：197720873]

00 00 00   //固定

//解密后

02 0D //固定

01 00

4A 79 38 4E 75 70 45 37 44 52 61 73 62 61 6A 49 //key0\_verifyee5验证

00 00 00 01 00 00 00 64 //固定

00 E4 00 03    //用在登录包中

4D 96 7B 44  //[ 时间：2011/4/2 9:26:28]

6F AD 4F D6  //[ IP地址：111.173.79.214]

00 00 00 00 00 00 00 00 //固定

00 D0 //token0\_verifye5 长度

2F 48 4C 8A C9 35 76 E3 70 1F 0D 20 81 28

B6 4C 12 84 2C DE 3B A9 8A 9D 3B 8F 18 A7 F5 BC

26 10 9F 4F A5 8C AC 79 08 3F 92 F0 34 AE A4 76

51 A9 D7 73 63 24 C5 BB B3 0B 52 F9 04 61 39 49

67 99 46 76 37 65 52 E6 3D 2B 29 26 D3 40 91 E1

4C 59 DD 70 B1 73 60 24 10 54 3E 11 79 E7 35 5A

5A EA E0 B6 7A EC 04 BE 9F 4E B8 AD 22 FF 01 DB

E0 AD B2 34 1F 90 B1 53 96 19 13 FD C3 C1 78 10

B6 CE 68 87 CD BC 0C 2C AC BD 75 5B D4 5A 69 86

7F B0 1A 53 AC CC 35 48 8C 3E 46 1D 21 6A F9 26

AD 4A 0D 4F A9 56 15 3D 46 34 9C 4C EB B0 EF 38

EE C7 74 63 75 7A 66 1C CF F8 E4 6E 53 0E 00 12

62 7E 03 07 38 D2 50 0B 57 83 A6 B3 31 36 2F E3

27 61//token0\_verifye5

4A 62 52 4E 6B 47 4D 7A 32 32 36 79 36 4E 51 6E //key1\_verifye5

00 78 //token1\_verifyE5 长度

00 01 4D 96 7B 44 00 70 F4 98 63 A4

54 BD FB 73 21 A0 6A 78 FA 34 50 B4 4D 56 A1 AF

EE 35 99 D7 BD 53 0F 0D B7 06 2B 58 E6 C9 74 E6

30 FB 3E C8 BF E6 BE 34 35 11 7B 02 CE 3D 20 5F

03 B1 32 F9 9B 67 4C CF 89 00 FE 30 81 1C BE 72

E4 3F F3 BF 6C 59 E1 35 2A C1 BC 14 B6 C6 E6 E0

D3 88 6A CA 36 49 67 4F E8 DF 7B F3 8C 06 A9 4D

8B A6 73 0E EA C7 F5 29 0D E0 63 3A //token1\_verifyE5

00 00 0E 02   //根据QQ版本固定

00 01

51 80 00 00 00 3C 00 02 //固定

00 73 //时间+token2\_verifyE5数据长度

01 //固定

4E 43 52 46 4E 73 58 62 56 65 6E 4D 58 65 49 4D //未知用途key

00 60 00 01 //固定

4D 96 7B 44//时间[ 时间：2011/4/2 9:26:28]

00 58 //token2\_verifyE5长度

E7 89 52 4B 12 AC 30 66 D7

D4 1F A1 7F 6C 86 C7 04 35 99 4B 03 D5 87 2D F4

C5 8E 76 EA 6A 15 13 26 6B 83 06 51 73 53 8D FD

04 1B 2E 9E FC 41 BE D5 E7 27 67 69 61 24 4F 91

08 23 90 90 A5 41 B8 03 79 35 7A 86 C2 02 5A 37

A8 6C E3 9D 58 AB 74 F7 A9 38 4F DC 68 05 C0 //token2\_verifyE5

00 00

]

[NO.9 2011-04-02 09:26:45 355 SEND]

02

21 07

00 E3

79 24

0B C8 FB 29

02 00 00 00 01 01 01 00 00 64 53

00 38 //token2\_auth 长度

23 C2 99 DA 27 32 FA 89

3C 85 CC C7 C0 40 50 6B 2F B9 7F B5 1A 5D AC D9

0A 5B FD 70 4B 67 1F 7A 96 47 7E 2D 20 56 84 29

03 EA B7 35 A3 01 ED 8F 65 93 D5 A0 6D F4 B6 72//token2\_auth

//密文-----------------------------------------------------

80 7D C8 39 BD 54 08 F1 F7 0D 6D 03 E0 3D 48 79

72 ED 41 7B FC 7D 31 8C 2A 86 51 C8 2C BE 34 89

33 CF E8 FC FF 0B B1 20 49 66 31 B9 AF 47 89 91

32 66 C7 78 0F BD EA A6 0B 4B 1C 7B 54 27 CD CA

30 5F 61 77 EB E7 CD 8A C3 30 2F AB ED E2 D7 B8

93 8F 3E E7 AD B9 F5 3A 85 6C BE 31 44 DF BD ED

99 44 D3 8A 37 54 5F 69 8B 79 D3 75 BD 9B 83 8A

5B AF FC 41 6B 19 F3 C4 DD 8E 0B D1 A0 71 F8 44

1D 2A C7 80 2A 96 42 CE 78 ED 23 B5 11 7F 08 03

45 01 5E D3 7A 36 41 6C BF 8F 46 C3 98 51 06 7D

6A 36 BD C8 D4 50 D0 27 88 25 CF F2 E1 16 87 9D

9C 9E 0A 58 13 D3 DC 0E 87 4C 92 41 D5 FF FF 41

7F 27 6C 23 70 BA F6 F3 F2 2D 8E 60 89 4F 92 C3

D8 5A B0 F8 3F B6 F0 9D B4 C8 75 48 AF 30 0C 68

63 7F 2F 1B 6E E9 EA 0F 6D F7 30 78 D2 42 5C 7E

02 0C 2C 39 E2 73 C1 B9

//end密文---用key2\_auth解密---------------------------------

--解密结果-------------------------------------------------

00 C8 00 01 00 00 08 04 01 E0 00 00 03 50 00 00

00 01 00 00 0C EB 00 38 6F 93 B7 CE 6E 78 57 23

76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43 A8 4F

D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB 50 54

1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1 70 71

00 78 00 01 4D 96 7B 44 00 70 F4 98 63 A4 54 BD

FB 73 21 A0 6A 78 FA 34 50 B4 4D 56 A1 AF EE 35

99 D7 BD 53 0F 0D B7 06 2B 58 E6 C9 74 E6 30 FB

3E C8 BF E6 BE 34 35 11 7B 02 CE 3D 20 5F 03 B1

32 F9 9B 67 4C CF 89 00 FE 30 81 1C BE 72 E4 3F

F3 BF 6C 59 E1 35 2A C1 BC 14 B6 C6 E6 E0 D3 88

6A CA 36 49 67 4F E8 DF 7B F3 8C 06 A9 4D 8B A6

73 0E EA C7 F5 29 0D E0 63 3A 00 00 00 20 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00

--end解密结果----------------------------------------------

03

///////////////整理/////////////////////////////////////

[

02 //包头

21 07 //固定版本号

00 E3 //命令

79 24 //命令序列号

0B C8 FB 29 //QQ号码[QQ号码：197720873]

02 00 00 00 01 01 01 00 00 64 53 //根据版本固定

00 38 //token2\_auth 长度

23 C2 99 DA 27 32 FA 89

3C 85 CC C7 C0 40 50 6B 2F B9 7F B5 1A 5D AC D9

0A 5B FD 70 4B 67 1F 7A 96 47 7E 2D 20 56 84 29

03 EA B7 35 A3 01 ED 8F 65 93 D5 A0 6D F4 B6 72//token2\_auth

//密文解密后的明文

00 C8 00 01 //固定

00 00 08 04 01 E0 //0x91data1

00 00 03 50 00 00 00 01 00 00 0C EB //0x91data2

00 38 //token\_captcha 长度

6F 93 B7 CE 6E 78 57 23

76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43 A8 4F

D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB 50 54

1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1 70 71//token\_captcha

00 78 //token1\_verifyE5 长度

00 01 4D 96 7B 44 00 70 F4 98 63 A4 54 BD

FB 73 21 A0 6A 78 FA 34 50 B4 4D 56 A1 AF EE 35

99 D7 BD 53 0F 0D B7 06 2B 58 E6 C9 74 E6 30 FB

3E C8 BF E6 BE 34 35 11 7B 02 CE 3D 20 5F 03 B1

32 F9 9B 67 4C CF 89 00 FE 30 81 1C BE 72 E4 3F

F3 BF 6C 59 E1 35 2A C1 BC 14 B6 C6 E6 E0 D3 88

6A CA 36 49 67 4F E8 DF 7B F3 8C 06 A9 4D 8B A6

73 0E EA C7 F5 29 0D E0 63 3A //token1\_verifyE5

00 00 //固定

00 20 //多少个填充位

///////////-固定32位0-////////////////

00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00

]

[NO.10 2011-04-02 09:26:45 382 RECEIVE]

02 //包头

21 07 //版本号

00 E3 //命令

79 24 //命令序列号

0B C8 FB 29 //QQ号码

00 00 00 //固定

////////////////////////密文/////////////////////

91 AA

A5 72 F2 0F 16 78 C6 3D 4F 19 94 4A 12 5D DB 63

3B 02 AE 25 38 B7 C9 70 E8 A5 A5 BA DE 6C C0 F8

48 BD 0D 49 51 5B 90 64 87 C0 DD B6 17 88

//end密文//////////////用key1\_verifye5解密///////////////

--解密后的明文-----------------------------------------

00 1B 00 00 12 01 53 //固定（qq号码不同则不同）

09 //QQ昵称长度

E7 9C 9F E7 94 B7 E4 BA BA //QQ昵称 utf-8码

01 //结果码

00 00 02 02 18 00 04 00 00 00 00 00 00  //固定

--end解密后的明文-------------------------------------

03

[NO.11 2011-04-02 09:26:45 733 SEND]           //这里要注意，这个是登录包了

02

21 07

00 30

52 53

0B C8 FB 29

02 00 00 00 01 01 01 00 00 64 53

00 38

23 C2 99 DA 27 32 FA 89

3C 85 CC C7 C0 40 50 6B 2F B9 7F B5 1A 5D AC D9

0A 5B FD 70 4B 67 1F 7A 96 47 7E 2D 20 56 84 29

03 EA B7 35 A3 01 ED 8F 65 93 D5 A0 6D F4 B6 72

//密文

43 C8 4A EF CF 93 E4 47 55 82 CC 39 D7 5B 2E 9B

5E D0 13 EA 0D 7C 6C 7D 82 1E 9E 44 62 24 64 C2

BE D6 66 8C 5D 96 CC EC D1 82 CF 71 CA C8 5F 41

45 4E 1D 30 F6 CB 84 6D BE D8 2B 9D D8 F3 90 80

A2 42 37 A3 A6 20 69 2A C5 74 94 52 F4 03 4C 1A

5A 00 12 47 FF BA F2 66 5D 23 5C 8D 95 5B EC E3

61 A2 05 84 14 ED 37 CF 67 8D B4 C6 34 F0 4B 4E

BD EB 11 8C F3 B7 DE CF 53 99 9C 75 84 94 1F 50

65 97 BA 6D 6B 5F 06 FF 7D EA 72 7B AE 1B 11 45

A4 B4 31 7C 7D 45 16 4F 62 94 D7 D1 C4 C8 01 27

E1 F3 F3 EF 92 E5 F2 FF 05 BD CE C1 42 F0 94 76

24 F3 7F 42 0B 72 F9 31 54 50 7D 9A 2F FE B1 EB

A7 85 67 80 1A 7E E7 04 A8 CD 23 57 42 7E A6 83

66 75 F0 8E A4 49 B3 56 C6 D3 EC E9 F4 CD 86 18

8C 31 35 85 C4 BF D4 A7 41 FC 51 D1 85 F8 F8 EB

51 89 B4 DE A6 17 F1 0C 5C 37 57 D9 E6 13 9F A1

DA 58 A3 59 7C C9 E8 CB 8F 6C 50 0F F2 F8 B0 DC

66 B8 E9 5D B0 C7 4D B2 44 A3 05 87 7C 7E E7 77

7C E2 52 3B 0A B7 E3 C5 67 BC 29 35 17 D1 77 5D

F2 DB 0B 9A 08 4C 71 74 34 9D 21 75 A7 F6 C4 5A

4B 6D 3F C4 C0 9B 36 AB 0B B7 55 A9 19 F5 54 F6

04 2B 91 E8 1A 44 5B 9B 67 C7 47 0C 9E 61 8A C2

67 23 D1 E6 41 FD 3C 4C 16 FD CC 8D 61 38 34 EF

D3 B7 7B 0C 3F E1 90 81 C1 60 80 32 95 C6 2C C3

38 6C DB 58 13 86 59 BD CB E7 E2 49 38 8D 92 C2

1D 44 B3 2E 2E 61 42 4C A5 79 86 45 BD 1C 35 44

8B BD E1 13 0E 71 01 24 96 F9 BF 9D 3B D5 10 FE

38 A3 28 11 FD 9E E4 03 F2 B4 94 3F 19 73 41 56

A5 16 CD 38 D3 AB 60 84 79 89 85 B5 7F 60 C7 CF

CC D1 20 B6 67 0B DD E9 BC B6 B5 DF 90 16 5E B2

4C EA 57 AF C8 E6 A8 C5 04 07 9A E4 54 D3 9C 0D

61 00 FA 6E A4 16 D2 81 3E 9E E3 55 3C 8E BD 3E

0A 9D AF B8 8C 15 A8 8D 7E BC B4 9A 28 CA 19 67

E4 3B A5 42 81 31 E2 78 E0 FB 4A 84 7D 0F E1 E2

01 6E A8 36 75 67 3B 59 4B 47 08 A6 5F CE 24 32

10 DB 86 D2 34 70 31 BD E9 22 09 AF C4 E4 35 21

35 2C 10 5E 40 57 1F A5 D0 A7 D3 73 C1 C7 DC 2A

B9 0B 48 DD 3C 27 D1 DD 20 78 F6 DF 30 81 7A F8

55 45 A3 47 1B E0 03 0A C3 01 3D 11 52 99 0E B6

CF 43 A4 73 6C 0F 6F 2E 94 77 B5 9F 91 2D 8E 37

A2 28 0B 98 69 C7 5F 0A A5 22 D3 5D 5E 96 16 3E

BC 6F 48 0A 7B 82 09 53 F5 74 F8 C5 95 F1 34 8F

5D F1 9C C4 42 64 DF 75 28 02 C4 4D 10 F2 27 52

77 B6 0A 20 91 17 40 25 41 24 FF 4B 9F 49 BF 35

AA B5 86 0B 8A 49 2E FE 7D 51 02 B5 5E 5F 0E D8

F2 96 69 70 F4 23 3C AF 47 0C 88 09 B7 E3 C3 6C

55 5F 57 AA 79 94 22 29 15 84 62 3B CD 30 85 45

//end密文

--解密后的明文------用key2\_auth解密--------------------------

00 01 //固定

00 00 03 50 00 00 00 01 00 00 0C EB //0x91data2

00 E4 00 03 //在E5的接收包里面未知的那个好像还是固定的

4D 96 7B 44 //前面的登录时间[ 时间：2011/4/2 9:26:28]

6F AD 4F D6 //在0x91包中的ip地址[ IP地址：111.173.79.214]

00 00 00 00 00 00 00 00 //固定8位0

00 D0 //token0\_verifyE5长度

2F 48 4C 8A C9 35 76 E3 70 1F 0D 20

81 28 B6 4C 12 84 2C DE 3B A9 8A 9D 3B 8F 18 A7

F5 BC 26 10 9F 4F A5 8C AC 79 08 3F 92 F0 34 AE

A4 76 51 A9 D7 73 63 24 C5 BB B3 0B 52 F9 04 61

39 49 67 99 46 76 37 65 52 E6 3D 2B 29 26 D3 40

91 E1 4C 59 DD 70 B1 73 60 24 10 54 3E 11 79 E7

35 5A 5A EA E0 B6 7A EC 04 BE 9F 4E B8 AD 22 FF

01 DB E0 AD B2 34 1F 90 B1 53 96 19 13 FD C3 C1

78 10 B6 CE 68 87 CD BC 0C 2C AC BD 75 5B D4 5A

69 86 7F B0 1A 53 AC CC 35 48 8C 3E 46 1D 21 6A

F9 26 AD 4A 0D 4F A9 56 15 3D 46 34 9C 4C EB B0

EF 38 EE C7 74 63 75 7A 66 1C CF F8 E4 6E 53 0E

00 12 62 7E 03 07 38 D2 50 0B 57 83 A6 B3 31 36

2F E3 27 61 //token0\_verifyE5

//35位0

00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00

67 87 C3 8F 95 EB 89 69 32 12 15 0A 94 AD 14 C6 //根据QQ版本固定

3A //未知随机

0A //登录模式oa正常 28隐身

00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 //根据版本固定

00 00 08 04 01 E0 //0x91data1

//16位0

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 38 //token\_captcha 长度

6F 93 B7 CE 6E 78

57 23 76 18 E7 D8 DC 7A 67 C8 FF 65 5A 2F 18 43

A8 4F D2 A6 09 09 94 21 58 EF E8 7A 44 B8 3A CB

50 54 1B FF CD 00 A6 86 CB E8 28 5C 45 BC 06 D1

70 71 //token\_captcha

00 00 00 08 00 00 00 00 08 04 10 00 01 40 01 CA //未知固定

18 88 64 00 10 10 B9 D4 75 E5 F1 12 11 F8 53 04 //未知固定

7C 5C C9 95 66

//25位0

00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00

02 16 37 69 27

00 10

76 58 5D 0D D0 A7 21 89 0A 65 CB F4 3B B4 65 8F

//249位0

00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

03

[NO.12 2011-04-02 09:26:45 761 RECEIVE]

02

21 07

00 30

52 53

0B C8 FB 29

00 00 00

//密文------------------------------------------

05 B4

5B 17 59 4A 05 82 4B 20 0E C2 B2 48 39 F7 59 04

55 33 5A 55 EB 29 C3 0D FC 49 6B 67 A2 EF 0C 82

96 A1 50 7D 37 88 04 04 30 A6 AC A5 CD 4B 8D E3

F1 DC 11 D3 7C 80 94 6B 5A 13 45 48 CB 5A E0 16

37 E6 B3 49 84 27 BA A3 94 24 C5 04 E6 48 FB 86

9E 44 A2 6A F2 9F 6B EF C1 A6 73 E4 B0 B8 77 A1

32 FF EC D9 EE 8D 32 A9 53 26 E1 3D B7 63 53 1B

56 74 4F C3 AD 52 7E C9 21 8C E8 4D EB F7 75 18

B2 38 AD A6 C7 4E 66 90 77 6D F4 51 29 8A C5 80

3A 86 ED 4D D9 F5

//end密文----------------------------------------------

--解密后的明文---用key0\_verifye5 但有时候会用key2\_auth---

00 59 7A 37 54 34 68 52 78 61 46 63 44 43 51 39

38 0B C8 FB 29 6F AD 4F D6 0F A1 4D 96 7B 45 00

00 00 00 03 14 8F FE 4F BB B6 63 C7 69 C3 F1 3C

DC A1 E8 76 A3 CD 17 F8 00 08 02 04 08 08 08 08

08 04 05 01 F4 03 E8 07 D0 0B B8 13 88 00 30 B5

79 37 25 56 87 D5 00 43 72 0E DF 20 2A 8E 37 61

8A 96 56 5B 30 2E 56 CE 2A E7 E3 2B 4C 7B CE 70

8B 91 82 25 87 00 85 E6 BA 01 31 5A A4 6E C8 79

0E 4A 74 71 6C 51 8B 00 00 00 07

--end解密后的明文--------------------------------------

03

/////////////整理//////////////////////////////

[

02 //包头

21 07 //版本号

00 30 //命令

52 53 //命令序列号

0B C8 FB 29//[QQ号码：197720873]

00 00 00 //固定

//解密后明文

00 //登录状态00登录成功

59 7A 37 54 34 68 52 78 61 46 63 44 43 51 39 38 //sessionkey

0B C8 FB 29 //[QQ号码：197720873]

6F AD 4F D6 //ip地址[ IP地址：111.173.79.214]

0F A1 //端口号4001

4D 96 7B 45//登录时间[ 时间：2011/4/2 9:26:29]

00 00 00 00 //固定

03 14 8F FE 4F BB B6 63 C7 69 C3 F1 3C

DC A1 E8 76 A3 CD 17 F8 00 08 02 04 08 08 08 08

08 04 05 01 F4 03 E8 07 D0 0B B8 13 88 //固定

00 30 //token\_login 长度

B5

79 37 25 56 87 D5 00 43 72 0E DF 20 2A 8E 37 61

8A 96 56 5B 30 2E 56 CE 2A E7 E3 2B 4C 7B CE 70

8B 91 82 25 87 00 85 E6 BA 01 31 5A A4 6E C8//token\_login

79 0E 4A 74 71 6C 51 8B //未知固定

00 00 00 07//固定

]

以上为QQ2011登录协议

**QQ2012 Beta 1 登录协议分析**

作者:　admin　　时间:　2012-07-09　　点击:　777次

[NO.1 2012-03-16 20:04:19 035 SEND 87字节]   
02 2B 27 00 91 2D A8 3B EB E4 1C 02 00 00 00 01   
01 01 00 00 65 35 AF 3E 99 E4 9F 8A A2 44 50 45   
4B FC 4F 16 AF 8C 18 B8 4C 1D 79 9B 08 42 76 1F   
F8 A2 6B A8 1C 27 CD 1F 25 44 2F D6 08 D1 7E E4   
60 54 5E DF 7C 8D 84 6F 35 38 D8 60 CB 74 BE C1   
1D AC 4E 1F 88 A7 03   
[   
02 //包头   
2B 27 //版本号   
00 91 //命令   
2D A8 //包序号   
3B EB E4 1C //QQ号码:1005315100   
02 00 00 00 01 01 01 00 00 65 35 //固定，QQ版本号不同则不同   
AF 3E 99 E4 9F 8A A2 44 50 45 4B FC 4F 16 AF 8C //0x91密钥   
00 01 //固定两字节   
00 00 08 04 01 E0 //0091Data01（在后面的命令里面要用到的）   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data02（在后面的命令里面要用到的）   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 //首次发送为15字节0   
03 //包尾   
]   
  
[NO.2 2012-03-16 20:04:19 350 RECEIVE 103字节]   
02 2B 27 00 91 2D A8 3B EB E4 1C 00 00 00 91 F9   
BD 15 D5 F9 AD 13 ED EA E2 52 81 5E 8B C7 00 3E   
1F F1 A3 7C 8D C5 6F 26 33 14 DD FD AE 64 5B 92   
37 66 21 C8 99 5E 85 75 F7 46 CB D8 D2 EA 1D C7   
0D BD 3F AA 27 D5 F2 19 FA 30 F1 24 75 80 3E 4A   
6A 37 E0 94 B6 4C 7E 2D AA 9B 34 20 D0 01 C8 3D   
37 4A BB AD 75 A0 03   
[   
02 //包头   
2B 27 //版本号   
00 91 //命令   
2D A8 //包序号   
3B EB E4 1C //QQ号码:1005315100   
00 00 00 //固定全为0   
00 //接触成功   
4F 63 2C 43 //登录时间:2012-3-16 20:04:19   
72 F9 D6 6B //登录IP地址:114.249.214.107   
00 00 00 00 00 00 00 00 //固定8字节0   
00 38 //0091\_Token长度：56字节   
F2 23 61 98 19 C0 AB 74 CF 06 98 C4 67 8B A9 B2   
28 65 33 8F 5D 59 77 47 94 4B 80 09 5E 4E 84 84   
51 56 81 30 35 97 9D B6 37 47 0B AF 41 3E B1 7D   
26 AD 3A 91 39 84 5E 80   
00 //接触成功   
03 //包尾   
]   
  
[NO.3 2012-03-16 20:04:19 351 SEND 199字节]   
02 2B 27 00 BA 3E A3 3B EB E4 1C 02 00 00 00 01   
01 01 00 00 65 35 29 58 26 59 D5 55 6E 07 7C 8C   
7F F0 B3 52 2E 21 BF 02 BE 9C 0F 90 2C F7 84 E9   
10 56 C2 18 BD 32 17 26 9F 0C 83 78 57 35 19 E0   
B4 AE A9 FB 24 AA 48 61 8B 4B 0D 52 F2 78 EE A1   
7A 4E 0E 7A 5C 35 DB 76 B5 0F A4 9A F2 BA 09 50   
E0 7C 85 87 EA C9 5C 9F 8A 6B 58 25 0F C2 67 32   
CD B0 92 62 44 85 D7 AE 15 8F 42 FA 61 C7 13 34   
21 67 96 F6 6F 89 78 2E 43 F3 45 64 6D 35 69 7F   
84 D1 E5 53 31 9F 51 C4 7B BE 74 53 0C 51 D7 5D   
07 79 4F FB 12 5E 8D 12 A6 EC 1C AD 2F C1 09 BB   
C5 74 BE EE 0F F2 FC 86 EC AA DA 66 5E 14 13 0D   
97 D8 BA A1 D4 18 03   
[   
02 //包头   
2B 27 //版本号   
00 BA //命令   
3E A3 //包序号   
3B EB E4 1C //QQ号码:1005315100   
02 00 00 00 01 01 01 00 00 65 35 //固定，QQ版本号不同则不同   
29 58 26 59 D5 55 6E 07 7C 8C 7F F0 B3 52 2E 21 //0xBA密钥   
00 01 //固定两字节   
00 00 08 04 01 E0 //0091Data01   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data02   
00 38 //0091\_Token长度：56字节   
F2 23 61 98 19 C0 AB 74 CF 06 98 C4 67 8B A9 B2   
28 65 33 8F 5D 59 77 47 94 4B 80 09 5E 4E 84 84   
51 56 81 30 35 97 9D B6 37 47 0B AF 41 3E B1 7D   
26 AD 3A 91 39 84 5E 80   
13 00 05 00 00 00 00 00 00 00 //固定   
00 38 //00BA\_New\_Token长度:56字节   
8B 02 49 59 55 16 0E 62 39 79 EA 2A 87 17 96 74   
FC 40 DC F8 22 D7 57 7A B1 A2 73 73 2A 37 C1 A5   
10 1F 43 8D 71 CC BC 73 F9 2A 53 C9 B0 B6 01 FD   
6F 43 AE FB 68 69 16 93   
03 //包尾   
]   
  
  
  
[NO.5 2012-03-16 20:04:19 434 RECEIVE 95字节]   
02 2B 27 00 BA 3E A3 3B EB E4 1C 00 00 00 4A 83   
46 98 94 4F 5F E9 C2 F6 5D 72 C2 F7 DA 00 85 8E   
C2 A5 2C 36 3A 40 E7 98 53 A8 04 C8 93 B9 F7 42   
82 9B 18 0F 55 2B 21 E5 78 55 53 6A 65 17 27 DF   
0B 15 90 B4 32 39 8A 0D D7 F6 CF 23 BB 38 3E 5C   
EB 8E 62 1E D8 C7 85 FB 57 76 A6 CB C7 90 03   
[   
02 //包头   
2B 27 //版本号   
00 BA //命令   
3E A3 //包序号   
3B EB E4 1C //QQ号码:1005315100   
00 00 00 //固定   
13 //验证结果：03或13表示成功，04表示需要验证码   
00 05 //固定   
00 //是否需要验证码：0不需要，1需要   
00 00 00 00 //验证码，需要验证码时为00 00 01 23，不需要时为全0   
00 38 //00BA\_Token长度：56字节   
7E 96 26 AA 51 0D 4F 89 25 3F C9 E9 A4 86 B4 84   
D3 02 C1 27 BC 6E C8 BD 34 DF 50 04 34 63 F9 11   
38 CE BC 34 C5 BC 96 84 C0 E8 B0 66 53 29 D7 CE   
D6 B0 DB E1 98 65 9F E6   
03 //包尾   
]   
  
  
  
[NO.8 2012-03-16 20:04:19 439 SEND 655字节]   
02 2B 27 00 DD 23 74 3B EB E4 1C 02 00 00 00 01   
01 01 00 00 65 35 D5 2F F0 73 0A 94 FB E2 45 88   
6A F7 28 BD 77 0C B8 20 17 E3 68 0C C0 9B 5F 19   
9E 50 8A 73 72 C6 B0 BA 9A C0 63 01 EE AB 55 05   
EE 2E 31 71 11 4A CC 9A F9 CC 83 85 59 AC 9C E1   
F1 93 F6 F9 D4 FF 53 E3 23 BF 53 D9 7E B3 E2 DA   
03 A3 02 C6 97 4B 0C D1 D1 71 DB F1 5C 2F 90 70   
76 FB D2 C0 59 92 79 BB CF 48 57 BA A8 F8 88 3A   
59 16 D0 79 F5 1D 66 72 C2 E5 FA 35 05 62 9A 75   
05 27 A8 3C 16 D4 F0 6B 45 33 70 0C 66 7F E8 9A   
86 0B AD A2 4D D0 7D 2E 51 42 E9 A3 4A 8F 47 33   
BC 02 A2 93 CE B0 0C 8A 41 A9 2F 71 83 2C F5 BF   
84 CC FB 94 BD 57 47 DA C5 CA 04 0B FA 91 48 C0   
5E 9A 1C 47 18 6C 35 46 37 51 7E 33 29 95 00 63   
32 13 26 E3 44 2C 67 F0 94 62 40 36 E5 F9 72 32   
11 4C 2A 74 CB F2 7E 39 D0 45 1B FB 7C 4E 3C 4E   
DA 08 C8 4B 50 1A 9B 91 9D 19 A0 CB 76 6C BF C0   
4D 1F 11 2D A4 1F 79 F4 60 C2 5A CA 8E 99 E7 42   
1A 49 74 F3 DE 77 A3 DF D0 D5 60 B3 5E 6F 3C E9   
45 7E 14 1C 87 17 72 F3 09 37 F8 F5 B5 55 18 B1   
59 97 23 50 6D B2 38 17 33 C4 CC C8 1B BA 0F 7A   
61 DC CF F1 27 47 43 B2 03 EC F0 37 23 2B CB DC   
78 54 F9 D4 6E C5 A4 01 25 6D 66 E7 DA 58 4F 8B   
34 63 AE 46 CF D8 E5 91 86 2C EC 1E 35 BD 18 CD   
28 50 06 DB DE 9B A1 EE 21 E2 24 F3 D2 1B A3 22   
90 D2 BA 6B C6 77 8D CE 87 EF 3C 91 AD 56 F5 81   
BA 3A DF DA 6C 54 51 04 61 7B 4D EB 04 7A EC EA   
6F CA AB 67 F8 60 41 30 FF 93 E7 06 FC B5 8C 43   
C2 2A E3 92 7D 73 DD 0F EE 6A 29 FB CE 0A C6 B9   
3E E0 F8 7E A9 54 53 51 5D BC FD 05 46 A6 B0 E8   
34 28 B9 63 A8 16 2A CA 89 A6 22 FA 6F 9F 2C 31   
44 13 C5 3F 95 FD 85 02 7B 2C 75 D5 10 31 46 E8   
B7 07 B4 43 33 2D 4A 8C 12 DA 33 95 DE D5 0F 27   
60 4D DF 2B 95 73 FE EA 08 D3 41 41 5D 5D BE BF   
42 C1 AC CA 8A 71 39 06 F4 A9 A0 42 56 31 F1 17   
84 27 33 8D 2A 59 AA E1 7D F8 80 10 E5 99 A8 A4   
49 74 85 8E A9 28 1B 41 88 53 F3 87 F4 02 55 F4   
41 91 DD EE 90 45 F4 0E 7D 22 D4 3A 7B B4 0D 74   
07 C3 7F E7 CF EC 6E D7 A9 80 24 9E A5 2B 84 91   
19 80 8E 57 33 A2 32 34 FE 51 CC A9 9A C3 2F FF   
E9 B8 BA E7 39 2D ED A7 F2 8D D9 73 90 1C 03   
[   
02 //包头   
2B 27 //版本号   
00 DD //命令   
23 74 //包序号   
3B EB E4 1C //QQ号码:1005315100   
02 00 00 00 01 01 01 00 00 65 35 //固定，QQ版本号不同则不同   
D5 2F F0 73 0A 94 FB E2 45 88 6A F7 28 BD 77 0C //0xDD初始密钥   
01 19 //固定两字节   
00 01 //固定两字节   
00 00 08 04 01 E0 //0091Data01   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data02   
00 38 //00BA\_Token长度：56字节   
7E 96 26 AA 51 0D 4F 89 25 3F C9 E9 A4 86 B4 84   
D3 02 C1 27 BC 6E C8 BD 34 DF 50 04 34 63 F9 11   
38 CE BC 34 C5 BC 96 84 C0 E8 B0 66 53 29 D7 CE   
D6 B0 DB E1 98 65 9F E6   
00 78 //密码验证：120字节   
71 34 78 8C 5C A4 C1 DC DA 99 CA 93 F7 5E 56 E6   
62 37 1D 6B 0C 5D B5 DE B1 6A 84 87 0A EE C3 D1   
90 A3 A8 3D 1C E2 26 4C 09 C7 F7 C3 A9 92 40 4E   
6F 4A D8 EB 33 1F 48 A6 3F 60 F1 D4 79 6B 5D B5   
F3 92 18 FF 9D FF 59 FA EB 6C 5A DA 0F 92 B7 30   
54 9F D8 4B D8 9B 8B 7B 58 25 0D BE F1 5D BC 16   
B1 99 CC 65 65 D9 A0 0B C8 DC FE 81 5B D3 57 7B   
88 86 F2 9B 96 15 F2 A7   
[   
92 E9 AF 29 //随机4字节   
00 01 //固定   
3B EB E4 1C //QQ号码:1005315100   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data02   
00 00 00 //固定3字节   
61 C2 E0 48 FA 94 78 C4 B3 1C BD C3 6E 20 42 B2 //密码的一次MD5值，服务器用该MD5值验证用户密码是否正确   
4F 63 2C 43 //登录时间：2012-3-16 20:04:19   
00 00 00 00 00 00 00 00 00 00 00 00 00 //固定13字节   
72 F9 D6 6B //IP地址：114.249.214.107   
00 00 00 00 00 00 00 00 //固定8字节   
00 10 //数据长度，16字节   
FD BA BA 81 12 83 74 47 B2 F9 B6 13 11 78 1D C8   
C9 5A 1E FA 93 80 65 01 52 93 39 CB 7F 8E B5 1B //00DD临时密钥(通过验证时客户端用该密钥解密服务端发送回来的数据)   
]   
00 14 //数据长度：20字节   
A9 D4 BC 8F 97 7A 80 48 A1 D3 AD 5C 0B 89 94 0B E3 4E 18 2D   
00 //固定   
00 38 //00BA\_New\_Token长度:56字节   
8B 02 49 59 55 16 0E 62 39 79 EA 2A 87 17 96 74   
FC 40 DC F8 22 D7 57 7A B1 A2 73 73 2A 37 C1 A5   
10 1F 43 8D 71 CC BC 73 F9 2A 53 C9 B0 B6 01 FD   
6F 43 AE FB 68 69 16 93   
01 3C 2E 01 //固定：4字节   
F3 CE 39 8A //固定：4字节   
00 10 //密钥长度：16字节   
AF 10 4B 99 7C 42 95 7F 7E 3D 69 A2 BA A6 BE F3 //0xDD固定Key1   
02 64 D2 0A 9D //固定：5字节   
00 10 //密钥长度：16字节   
BA 5D 3D 29 C7 31 94 C9 52 18 84 83 60 9E 50 2E //0xDD固定Key2   
//尾部填充0   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00   
03 //包尾   
]   
  
  
  
[NO.10 2012-03-16 20:04:19 521 RECEIVE 319字节]   
02 65 35 00 DD 23 74 3B EB E4 1C 00 00 00 58 A6   
D6 C5 C2 F5 05 52 F6 53 09 6E 86 89 93 99 CE D2   
92 4D 27 CB 6E 10 0F 6C C8 78 B0 3F 02 69 C9 DA   
45 72 E6 F0 D0 5E 65 C0 02 FC F7 4F 48 B4 AC 29   
EA DB 1A A5 C1 97 EB DB 7C 22 88 96 6B 46 A6 D5   
F0 40 61 48 D5 3B C5 12 B6 8A 53 92 83 F1 0B B1   
3C 4D AF 16 3C 2B 2E 23 9E A5 20 8E B8 82 D5 36   
88 AB 5F 2E E6 4E 39 3A BF 28 C4 DE EE E7 71 F4   
B9 C0 FE CE C4 03 46 54 B5 23 CB 9A 25 AB 86 E8   
56 90 19 09 97 09 5F 62 94 BE 6E 55 C8 00 A1 27   
AC 18 33 11 56 CB BC 67 17 4E 7D 26 E3 28 06 7C   
0D 2A 8E F8 BF 1A 7A 81 13 5C CC 67 87 00 CA FE   
1B B5 5F 31 45 FE 4A 7D F6 52 AB 84 9F 1E 2E DF   
B1 47 DC 03 0B 1D DE DB 6B D3 34 CD CD 30 17 D4   
68 4E D6 E0 F9 BA 1C C5 E7 0A 36 E2 00 D4 E8 D4   
4D F6 01 A1 88 C9 4B 66 45 5B 43 B5 F0 24 7C 20   
68 56 CC 3B C7 E5 A7 97 7D A4 CA 89 50 C4 0A BD   
51 69 4E 46 F2 72 78 33 C3 35 67 78 C5 59 FD C2   
29 E7 A8 19 DD 3F 35 F8 E8 DD C4 4A 0A FA 5E 48   
0A 8F D2 51 90 8F D7 37 F1 F9 FB D1 F0 BF 03   
[   
02 //包头   
65 35 //版本号   
00 DD //命令   
23 74 //包序号   
3B EB E4 1C //QQ号码:1005315100   
00 00 00 //固定全为0   
01 1B //数据长度   
00 //成功，（00验证通过、33或51拒绝登录、BF没有该QQ号、34密码错误）   
00 20 //00DD\_Token1，长度：32字节   
13 2A C4 FA 2B 9E B2 C1 40 DF 26 BF 88 AC 2B C0   
36 27 C5 46 90 71 42 64 91 66 97 9F 26 8E E9 65   
00 98 //数据长度:152字节   
00 02 //固定   
4F 63 48 64 //登录时间：2012-3-16 20:04:20   
00 90 //00DD\_Token2数据长度：144字节   
52 36 78 76 E1 0B 22 D8 5C 9F D3 0A 5B AF 2C 98   
CD D7 7F 08 25 9F E9 62 16 F0 EC A6 00 C2 0B 1C   
23 F3 A6 5E E1 C0 54 0B F6 27 17 E4 80 5E 0F 46   
A8 86 B4 3B C9 5E B3 AE FA 43 7D 03 E9 D7 FA D5   
F6 00 FE BA D1 6F CE FD A2 8C 1E 8E 08 F5 25 08   
F9 A0 D9 89 D0 2B 1B 85 8A 26 B5 DD 15 BA 60 27   
49 2E 06 7F 8A F9 6A 42 DE 9E 42 5A 4B 1E 8D 3A   
16 70 3F 2D 99 E5 1D 87 18 87 00 62 14 AB 87 AB   
12 32 26 E4 05 F3 06 1A 3C 03 75 B0 53 BD 6C 9C   
00 38 //00DD\_Token3数据长度：56字节   
DA 97 CF 17 6D 1F 99 33 E8 49 A6 25 70 7D 61 91   
91 B2 15 A9 D9 BD 6D 13 7A 8F 14 14 A1 55 D4 EE   
15 7D 37 09 48 FC 90 5F 3A CD 3C 15 29 00 BF FC   
AB 09 39 FC BD 62 E5 C1   
54 51 4B 35 43 77 6A 59 76 68 78 48 75 49 41 7A //00DD\_Key1   
00 00 //固定   
3A 42 5B 25 5B 7B 5A 7E 47 5A 77 70 6A 25 5F 67 //00DD\_Key2   
00 00 //固定   
03 //包尾   
]   
  
[NO.11 2012-03-16 20:04:19 521 SEND 369字节]   
02 2B 27 00 E5 70 79 3B EB E4 1C 02 00 00 00 01   
01 01 00 00 65 35 00 38 DA 97 CF 17 6D 1F 99 33   
E8 49 A6 25 70 7D 61 91 91 B2 15 A9 D9 BD 6D 13   
7A 8F 14 14 A1 55 D4 EE 15 7D 37 09 48 FC 90 5F   
3A CD 3C 15 29 00 BF FC AB 09 39 FC BD 62 E5 C1   
69 5D 60 C4 0C C3 A0 EC 47 B5 72 A7 77 A6 B4 E3   
B3 42 C6 B7 57 1A C6 84 DE 9E D7 7D 1B 48 A9 1E   
D6 E9 B1 C7 D8 2F 01 89 3B 3E C6 E3 81 23 F1 2C   
71 4C E3 D8 39 EA 43 DB 6D BD 87 8C 41 A2 22 DB   
A9 20 8F 6A B5 4B 6D 88 EF AA 6F BB 42 D3 CB 7F   
06 AF 60 24 26 E9 BA E1 4D 2D C3 49 45 6F FE 65   
9C 88 64 EF 12 6B 17 89 3B AB 78 A6 2B 28 B9 E6   
EB DF BD E0 63 FF C3 54 D8 36 DD F9 5A 6A 61 6D   
F4 61 86 4E 1C FF 4A CE C5 55 6B A4 F6 F9 BE 6C   
99 3E 15 4E 1F 22 17 90 37 5C CD 9F 18 BB FD 28   
47 80 8E 7F 44 1A FC F1 86 2A 3C 68 0B 2A EE C6   
B4 56 65 79 E7 FF 2A 19 71 8A 2F 69 91 F8 A6 50   
7D D0 09 EC 49 6E F9 3C A8 77 42 D5 C0 A3 DF 2A   
6F 62 41 7D C9 D5 9E 0F 8F 30 CC F5 92 B6 5F 85   
80 89 85 34 F0 EA A4 BB 6B 8B BA C2 37 31 74 C3   
BF EE 63 C4 F5 80 AC 1C 56 9C 09 C5 2C 91 EC 73   
09 1C 50 3D 16 4D C9 27 65 C7 1F 0C 05 87 BD F8   
40 45 FF F5 69 65 59 8B 05 C0 FD E8 09 A6 D6 A8   
03   
[   
02 //包头   
2B 27 //版本号   
00 E5 //命令   
70 79 //包序号   
3B EB E4 1C //QQ号码:1005315100   
02 00 00 00 01 01 01 00 00 65 35 //固定，QQ版本号不同则不同   
00 38 //00DD\_Token3长度：56字节   
DA 97 CF 17 6D 1F 99 33 E8 49 A6 25 70 7D 61 91   
91 B2 15 A9 D9 BD 6D 13 7A 8F 14 14 A1 55 D4 EE   
15 7D 37 09 48 FC 90 5F 3A CD 3C 15 29 00 BF FC   
AB 09 39 FC BD 62 E5 C1   
01 0E 00 01 01 //固定   
00 00 08 04 01 E0 //0091Data01   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data02   
00 38 //00BA\_Token长度：56字节   
7E 96 26 AA 51 0D 4F 89 25 3F C9 E9 A4 86 B4 84   
D3 02 C1 27 BC 6E C8 BD 34 DF 50 04 34 63 F9 11   
38 CE BC 34 C5 BC 96 84 C0 E8 B0 66 53 29 D7 CE   
D6 B0 DB E1 98 65 9F E6   
00 20 //00DD\_Token1数据长度：32字节   
13 2A C4 FA 2B 9E B2 C1 40 DF 26 BF 88 AC 2B C0   
36 27 C5 46 90 71 42 64 91 66 97 9F 26 8E E9 65   
00 98 //数据长度:152字节   
00 02 //固定   
4F 63 48 64 //登录时间：2012-3-16 20:04:20   
00 90 /00DD\_Token2数据长度：144字节   
52 36 78 76 E1 0B 22 D8 5C 9F D3 0A 5B AF 2C 98   
CD D7 7F 08 25 9F E9 62 16 F0 EC A6 00 C2 0B 1C   
23 F3 A6 5E E1 C0 54 0B F6 27 17 E4 80 5E 0F 46   
A8 86 B4 3B C9 5E B3 AE FA 43 7D 03 E9 D7 FA D5   
F6 00 FE BA D1 6F CE FD A2 8C 1E 8E 08 F5 25 08   
F9 A0 D9 89 D0 2B 1B 85 8A 26 B5 DD 15 BA 60 27   
49 2E 06 7F 8A F9 6A 42 DE 9E 42 5A 4B 1E 8D 3A   
16 70 3F 2D 99 E5 1D 87 18 87 00 62 14 AB 87 AB   
12 32 26 E4 05 F3 06 1A 3C 03 75 B0 53 BD 6C 9C   
00 00 01 00 00 00 00 //固定   
03 //包尾   
]   
  
  
  
[NO.14 2012-03-16 20:04:19 595 RECEIVE 575字节]   
02 2B 27 00 E5 70 79 3B EB E4 1C 00 00 00 74 DC   
36 A3 34 C0 6C 78 8A 22 68 41 C6 1B 8D 83 FF 2A   
B3 32 9A 05 C0 DB 91 C5 50 B1 0C C1 45 FB A6 45   
48 25 AB 77 17 50 D1 0E 0F 47 D5 AC E1 EE 6A 62   
88 8E 3D 0F 27 0B 98 8F F5 A6 80 BB AD A1 BD 9D   
62 4B 8B AC 22 51 35 F2 ED 72 2A 16 C7 13 ED 46   
56 73 90 1E 2B 5B 00 86 F6 F1 84 45 BD 60 03 79   
8B A7 22 83 38 5C D9 F5 2E 49 9C 6D 3D B7 2F 55   
F8 FD 10 44 C6 2F 9D F7 3F B6 7D 9A 7C 62 96 D6   
60 35 15 C7 F3 9D 03 93 8B E1 F8 90 82 51 C1 AD   
36 E5 B3 FC 2C FC 45 94 72 DF B2 26 85 3D 34 EE   
7C FA B9 F5 A0 31 3E 96 5B 78 33 EB 24 75 C5 7E   
1E 2E 40 74 71 AE AB C5 CC 85 50 CE 5F A7 66 13   
F1 86 C0 3F A2 06 A0 C5 F0 D8 11 54 88 9B 3A 0E   
A0 CB 18 AF 64 74 33 36 42 DF A9 EA 4C 08 43 9C   
F2 98 A7 90 E8 50 78 B2 B0 4A 39 02 44 18 66 AB   
51 CF F8 8C 8B 6D 12 5F 5E 70 6D 34 5D 3D 7C 76   
A5 53 01 C5 33 FF 20 F6 ED 0E 84 2A 6E EB F7 D0   
92 A6 2F 7C 02 61 2E 2E 82 9F CD FD 7F 88 39 91   
AA 42 88 4F AC 72 0F 3C 1D D6 76 1C E0 DB B6 26   
AE E9 8C 7A AE 1F 11 BE A3 AF 7F 3C 9B F3 9D D8   
4B 9C 9A 2B AF 1C 3F B7 41 9E 3A A9 A6 0A 14 B1   
75 52 0B BC 48 D6 82 A9 8F 9C 9F 99 EA DA 74 E3   
5B D8 B6 29 29 A3 DA EF F1 68 0F EF 33 18 F3 0D   
4A 4E 02 51 8C E7 1E 5E DB DC 90 C3 35 6E 63 0D   
C0 49 96 3B 90 7D 4D 61 84 7B 82 C9 3E D2 90 2E   
36 83 F0 08 77 D6 B0 1A 27 41 2D 4A 7F 0F F9 DA   
33 41 61 4F 23 CB 76 10 9C 0D 01 2B E1 12 4C 86   
ED 5B 81 11 01 D2 20 41 2E 59 B1 98 B1 C9 FD 0F   
8D 0F 32 F0 63 E7 04 4F 53 56 CD BD 45 EB 1A A1   
3A FB 12 27 7E EB B3 DA BD 80 B3 38 0D E1 8B A4   
E9 D1 DD 6F 64 77 24 9D EF 04 C4 51 C3 60 8B 3C   
A2 F3 93 3C EF 1D 2D D1 44 DA 60 6B D8 AC C6 51   
DC C3 BE D5 1A A5 78 A3 DF 9B 04 FF A6 B5 7C EE   
24 D8 A8 F5 1A 64 12 35 D0 49 44 8C 4D 46 F2 CB   
FD 84 70 C5 2B 25 18 2B CF 17 E2 95 F6 B9 03   
[   
02 //包头   
2B 27 //版本号   
00 E5 //命令   
70 79 //包序号   
3B EB E4 1C //QQ号码:1005315100   
00 00 00 //固定全为0   
02 1D //QQ号不同则不同   
01 00 //固定   
27 2A 63 56 3F 2D 54 52 3D 2A 2B 42 79 25 7B 68 //00E5\_Key1   
00 00 00 01 00 00 00 64 //固定   
00 E4 00 03 //固定   
4F 63 48 64//登录时间：2012-3-16 20:04:20   
72 F9 D6 6B//登录IP：114.249.214.107   
00 00 00 00 00 00 00 00//固定   
00 D0//00E5\_Token1长度：208字节   
45 C8 A8 D5 FE 4B E0 95 8D CA 62 4E 97 EF 2C 52   
0F 07 D4 71 E0 5B AB D3 46 E7 3D 60 9F DC 8E 30   
87 22 AB 9B 3B 30 93 35 59 F0 28 1F 5F 06 B9 10   
C8 93 D9 63 24 07 46 2C 19 6E 03 0C 64 3F E6 D3   
17 AC 5D D0 28 49 68 57 14 A3 E9 D9 27 A3 B7 38   
5F C0 5A A8 A5 D3 6B B6 80 5D 7F ED FB 9A 0E 05   
B9 02 AF 94 57 DF C1 84 F6 B8 AA 8F 50 7F 77 9F   
00 3B EE EE 2F C9 8A 06 4A C6 B3 67 FE DD 60 50   
77 1D 8D A6 59 22 D1 97 34 94 43 77 47 67 A4 28   
4E 67 10 69 36 37 68 07 EF 7B E4 7C 9E 1F 52 E2   
6F 9E 36 F1 80 C6 C5 1B 96 16 8B 78 3B 92 38 E3   
45 6B A6 67 43 0F 7D 90 77 57 33 FE D0 D9 6E A6   
66 0C DF 4F D9 69 7A 18 53 7A 76 DF AA 1C F9 CC   
79 42 3A 5A 34 5F 6D 3A 3E 6E 4A 7E 25 77 5E 70 //00E5\_Key2   
00 78//00E5\_Token2长度：120字节   
00 01 4F 63 48 64 00 70 96 42 B8 E0 0B 69 84 60   
A0 7D 75 05 95 75 09 77 8B F6 B9 6E BF C5 19 1D   
54 E5 08 AD 9D 7F 8E AE 9D 99 99 39 BB 27 B3 BB   
14 34 B7 40 03 65 8F 7F CE 88 2F 00 5D F6 C6 21   
9F 83 BF 0C 5D E2 6C EA 6E 44 85 FB 2A C6 5C EA   
B5 C8 3F 59 A3 3F E5 D8 48 88 B2 E7 1B DB 01 DD   
E1 C7 C3 BF 8F 2D DF A5 EC 1F 67 BA 38 35 0A 62   
4A 46 E4 B5 36 E9 B2 76   
00 00 0E 07 //版本不同则不同   
00 01 //固定   
51 80 00 00 00 3C 00 02 //固定   
00 83 //接下来数据长度：131字节   
01 //固定   
21 62 55 41 7A 38 56 45 32 28 6B 69 74 63 64 56 //Key   
00 70 00 01 //固定   
4F 63 48 64 //登录时间：2012-3-16 20:04:20   
00 68 //00E5\_Token3长度:104   
6D 4E 82 DE BF 2B 1A C7 26 83 9F 85 79 8C BE 68   
4D E8 70 B7 19 B0 BF 55 16 2A 7D 5B 54 F5 50 C9   
16 36 22 37 20 73 FF E0 0E 7C 8F 91 BC 13 F9 3B   
33 BF 6F 13 9A 8F 7C D0 99 F6 C1 FF AE 6B 97 2E   
69 28 BB 13 D4 99 F1 8F 5F 4C 08 69 8E F4 81 B1   
05 91 16 E3 88 5B 12 BA 25 14 DC 24 69 6F C4 E7   
18 D7 47 BF C4 A4 BB 7B   
00 00 //固定   
03 //包尾   
]   
  
  
  
[NO.16 2012-03-16 20:04:19 596 SEND 329字节]   
02 2B 27 00 E3 14 9D 3B EB E4 1C 02 00 00 00 01   
01 01 00 00 65 35 00 38 DA 97 CF 17 6D 1F 99 33   
E8 49 A6 25 70 7D 61 91 91 B2 15 A9 D9 BD 6D 13   
7A 8F 14 14 A1 55 D4 EE 15 7D 37 09 48 FC 90 5F   
3A CD 3C 15 29 00 BF FC AB 09 39 FC BD 62 E5 C1   
1A ED 6D 58 0A 64 04 DB 89 DF 4A D6 78 AA 22 82   
4C FC C5 26 93 B6 32 2C 95 8B AC 89 E5 AD 00 ED   
A5 1E 4C 97 1B 9B 65 92 39 02 26 10 63 91 D5 50   
9C DE 89 75 98 C8 CF CB 59 91 3E 43 BA 71 E2 FE   
DC B9 F9 33 03 85 91 7E 84 EF B0 BE EC 8D E7 67   
AB 8C 98 2F 2E E9 B0 58 ED EA C1 97 70 D1 82 55   
D4 55 BC AA 52 FA 26 12 B7 11 E9 CD 2B 33 6F CE   
9E 42 D5 ED 89 E8 D0 A0 34 56 DE 3E 63 60 74 B1   
5F FE 8A 27 7E C0 DA 98 4D 12 08 90 BB C2 FB 9F   
6C 10 DE A7 C7 2A 9E B9 9E 10 C0 2A 14 92 08 6C   
77 42 0A 66 E5 D2 53 81 79 74 78 5F D6 C1 5F 93   
84 12 6F E2 68 44 A0 2E 00 11 15 B1 09 A1 CB DE   
BD 1F 51 07 68 E1 B2 79 F1 37 6E 98 D8 17 F4 30   
0D AA D0 37 91 8A DC EA A9 5A 96 FB 65 1D 73 46   
A4 09 C4 49 DA 69 13 17 4F 4D 8E A0 B1 D2 B2 12   
5A DB 61 AF 6D 4F 3D 0F 03   
[   
02 //包头   
2B 27 //版本号   
00 E3 //命令   
14 9D //包序号   
3B EB E4 1C //QQ号码:1005315100   
02 00 00 00 01 01 01 00 00 65 35 //固定，QQ版本号不同则不同   
00 38 //00DD\_Token3长度：56字节   
DA 97 CF 17 6D 1F 99 33 E8 49 A6 25 70 7D 61 91   
91 B2 15 A9 D9 BD 6D 13 7A 8F 14 14 A1 55 D4 EE   
15 7D 37 09 48 FC 90 5F 3A CD 3C 15 29 00 BF FC   
AB 09 39 FC BD 62 E5 C1   
00 C8 00 01 //固定   
00 00 08 04 01 E0 //0091Data1   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data2   
00 38 //00BA\_Token，长度：56字节   
7E 96 26 AA 51 0D 4F 89 25 3F C9 E9 A4 86 B4 84   
D3 02 C1 27 BC 6E C8 BD 34 DF 50 04 34 63 F9 11   
38 CE BC 34 C5 BC 96 84 C0 E8 B0 66 53 29 D7 CE   
D6 B0 DB E1 98 65 9F E6   
00 78 //00E5\_Token2，长度：120字节   
00 01 4F 63 48 64 00 70 96 42 B8 E0 0B 69 84 60   
A0 7D 75 05 95 75 09 77 8B F6 B9 6E BF C5 19 1D   
54 E5 08 AD 9D 7F 8E AE 9D 99 99 39 BB 27 B3 BB   
14 34 B7 40 03 65 8F 7F CE 88 2F 00 5D F6 C6 21   
9F 83 BF 0C 5D E2 6C EA 6E 44 85 FB 2A C6 5C EA   
B5 C8 3F 59 A3 3F E5 D8 48 88 B2 E7 1B DB 01 DD   
E1 C7 C3 BF 8F 2D DF A5 EC 1F 67 BA 38 35 0A 62   
4A 46 E4 B5 36 E9 B2 76   
00 00 //固定   
00 20 //数据长度：32字节   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
03 //包尾   
]   
  
[NO.17 2012-03-16 20:04:19 672 RECEIVE 71字节]   
02 2B 27 00 E3 14 9D 3B EB E4 1C 00 00 00 93 B1   
CA 67 41 8B 5D 2A 90 22 CD 4E 43 0C 5A CA 8F 17   
A6 5C 75 4F CC FD 9D 14 13 2A 2E 44 08 7F 79 FF   
4F 08 A7 99 A0 9D 32 95 63 27 28 B6 53 23 20 B1   
03 CC 8B 46 AB EB 03   
[   
02 //包头   
2B 27 //版本号   
00 E3 //命令   
14 9D //包序号   
3B EB E4 1C //QQ号码:1005315100   
00 00 00 //固定全为0   
00 24 00 00 1B 00 00 //固定（QQ号不同则不同）   
12 //昵称长度：18字节   
E4 B8 A8 E4 B8 B6 E7 81 AC E9 A3 8E E5 90 AC E9 9B AA //用户昵称：丨丶灬风听雪   
01 //结果码   
00 40 02 00 19 00 04 00 00 00 00 00 00 //固定   
03 //包尾   
]   
  
[NO.18 2012-03-16 20:04:19 719 SEND 857字节]   
02 2B 27 00 30 2C D6 3B EB E4 1C 02 00 00 00 01   
01 01 00 00 65 35 00 38 DA 97 CF 17 6D 1F 99 33   
E8 49 A6 25 70 7D 61 91 91 B2 15 A9 D9 BD 6D 13   
7A 8F 14 14 A1 55 D4 EE 15 7D 37 09 48 FC 90 5F   
3A CD 3C 15 29 00 BF FC AB 09 39 FC BD 62 E5 C1   
48 9C 69 D3 22 A0 6E F9 6B 7C E9 2B 58 92 52 4F   
29 DB 3E 99 33 07 07 CE 85 CF 80 55 5D 9B 52 AC   
D5 6F 14 76 4D 0A 05 A6 D1 12 69 55 63 77 45 DA   
CD C5 08 49 7A 40 A9 71 9E 19 6F FE 83 F7 1D EB   
37 16 17 27 B9 0F 5C 87 9F 56 88 5F D3 D0 B8 11   
22 86 B4 E5 AC 61 7F 9E F5 D1 B3 EA F9 72 4D 2F   
A4 D8 A7 1F 93 93 D0 08 9D 24 13 DD 25 84 F1 78   
21 60 2A 30 CE 30 0A B8 A8 B7 FE 71 BA 76 6D 40   
3F B6 6E F8 4C D9 27 4A 29 C1 46 DB 92 A2 D1 74   
A5 59 BC F8 A2 24 81 C2 10 74 FE AC 89 E3 89 0A   
59 E2 44 16 15 A5 AB C2 0F 4B 76 35 78 59 FD FA   
D1 C2 BA 23 BE CB 8B FA EA BA 56 31 64 A6 D0 57   
A3 24 4D 1A 02 22 D7 D5 FB 94 69 DA 2B E7 58 A9   
73 B3 11 DA D5 A3 C7 CE 05 56 B4 EC B5 20 FF 3E   
06 31 B3 4B 09 C9 EF 94 32 AB 6B EF 2D AD D5 5F   
96 88 C3 98 02 BF 7B B9 45 FD 2F 5E FF 8A AA FC   
45 1E EB F6 BC 45 CF 5B 14 14 93 93 D2 95 0C 54   
93 B3 42 2E 99 9A 19 7A 15 16 EE 3C 3D 82 34 15   
AD 03 D6 A8 B3 52 07 2C 3C D6 A8 F9 C0 8E 28 53   
6F F7 36 3D A7 A9 92 2F 6B 28 71 C9 E4 2F 6B ED   
37 3C 1A 69 98 48 29 93 F9 EB 50 38 3B 2F A9 9D   
6E A2 CD 07 09 44 45 A8 FF C4 22 93 87 41 8B 41   
4E 61 43 48 A3 FA 3E 76 EE 18 88 7A 52 22 BC 85   
A9 B4 CE 1B 73 C0 C4 57 FA CB E6 B7 9F E3 4B 81   
33 08 FD EA EF 8E CD 89 4E 29 71 B5 DC CA ED BA   
AD 81 FA A6 C6 AD AF 66 11 9A E0 F8 B2 98 49 9D   
F1 BD 8E 61 FB 4A 48 F1 F5 7C AD 3C F6 91 9E C4   
A7 1E 9C E7 77 0E 77 2D 3B 6C D9 8D C8 53 1F 59   
D0 F0 FF D0 1C B0 0D B8 6D D5 7C 65 AC 78 89 E3   
5A F6 6C A9 FB DD 8A 00 59 BB C7 91 13 1D 46 18   
0F 5E 0D B6 C4 88 51 C8 91 E6 D7 A7 04 C2 3E 97   
D6 D6 3B 85 EC CA 8F 3A 09 91 B4 F5 B3 B2 50 2C   
2F 1A 7F BF 95 E2 FF 48 2D CB BA 26 9F B0 FC 55   
F4 AD 19 A6 C2 B2 EA 2C 8A 0F FE 16 AD FE 4D EB   
0C 1B 02 0B 7B E0 85 F6 36 21 B4 E5 DF 0C 74 91   
E8 59 53 87 7E 76 34 46 43 14 44 9C 8A 40 73 94   
65 6D 43 82 92 87 B1 4B AA 61 A5 96 2F DD 5D 97   
47 D2 DB 84 A7 B0 AD FD 3F FF 4A 55 5F 32 3E FD   
20 E8 1C 74 F6 9C 86 C9 C1 01 85 16 66 81 9D EF   
DB EB 0D CB 06 82 4B 88 3B EE 89 CB 57 09 8F 08   
1F 7B 97 83 EC F8 5E 34 A6 8E A2 AB B6 96 36 A1   
67 A8 13 70 7D 94 27 D0 CA F8 7D 9C DC C7 F3 07   
0D 0B B5 B4 01 21 23 20 37 51 D1 27 86 DA 2D FD   
D8 28 F0 46 79 D7 D2 FF F3 15 7F CB D5 D5 92 88   
6C D8 45 AF 49 05 EF 14 40 41 61 72 1D E3 C8 62   
E9 88 58 6F 9C C0 17 B0 C0 8B 6A 63 5C A3 50 3E   
6A 15 BC 3C 87 FF 4F 42 50 00 C9 C2 8B F8 18 0F   
72 20 47 B3 85 8B BB 2E 82 38 3D 21 38 34 2C C2   
35 66 50 35 25 C3 6B A4 03   
[   
02 //包头   
2B 27 //版本号   
00 30 //命令   
2C D6 //包序号   
3B EB E4 1C //QQ号码:1005315100   
02 00 00 00 01 01 01 00 00 65 35 //固定，QQ版本号不同则不同   
00 38 //00DD\_Token3长度：56字节   
DA 97 CF 17 6D 1F 99 33 E8 49 A6 25 70 7D 61 91   
91 B2 15 A9 D9 BD 6D 13 7A 8F 14 14 A1 55 D4 EE   
15 7D 37 09 48 FC 90 5F 3A CD 3C 15 29 00 BF FC   
AB 09 39 FC BD 62 E5 C1   
00 01 //固定   
00 00 03 63 00 00 00 01 00 00 10 F3 //0091Data2   
00 E4 00 03 //固定（00E5中接收）   
4F 63 48 64 //登录时间（0091中接收）：2012-3-16 20:04:20   
72 F9 D6 6B //IP地址（0091中接收）：114.249.214.107   
00 00 00 00 00 00 00 00 //固定   
00 D0 //00E5\_Token1长度：208   
45 C8 A8 D5 FE 4B E0 95 8D CA 62 4E 97 EF 2C 52   
0F 07 D4 71 E0 5B AB D3 46 E7 3D 60 9F DC 8E 30   
87 22 AB 9B 3B 30 93 35 59 F0 28 1F 5F 06 B9 10   
C8 93 D9 63 24 07 46 2C 19 6E 03 0C 64 3F E6 D3   
17 AC 5D D0 28 49 68 57 14 A3 E9 D9 27 A3 B7 38   
5F C0 5A A8 A5 D3 6B B6 80 5D 7F ED FB 9A 0E 05   
B9 02 AF 94 57 DF C1 84 F6 B8 AA 8F 50 7F 77 9F   
00 3B EE EE 2F C9 8A 06 4A C6 B3 67 FE DD 60 50   
77 1D 8D A6 59 22 D1 97 34 94 43 77 47 67 A4 28   
4E 67 10 69 36 37 68 07 EF 7B E4 7C 9E 1F 52 E2   
6F 9E 36 F1 80 C6 C5 1B 96 16 8B 78 3B 92 38 E3   
45 6B A6 67 43 0F 7D 90 77 57 33 FE D0 D9 6E A6   
66 0C DF 4F D9 69 7A 18 53 7A 76 DF AA 1C F9 CC   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00   
85 CF 93 C1 56 93 B8 D0 9B D0 22 92 2D FF 9A CB //固定   
AE //随机一字节   
0A /提交登录状态   
//固定   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00   
00 00 08 04 01 E0 //0091Data01   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 //16字节0   
00 38 //00BA\_Token长度：56字节   
7E 96 26 AA 51 0D 4F 89 25 3F C9 E9 A4 86 B4 84   
D3 02 C1 27 BC 6E C8 BD 34 DF 50 04 34 63 F9 11   
38 CE BC 34 C5 BC 96 84 C0 E8 B0 66 53 29 D7 CE   
D6 B0 DB E1 98 65 9F E6   
//固定   
00 00 00 08 00 00 00 00 08 04 10 00 01 40 01 F3   
CE 39 8A 00 10 AF 10 4B 99 7C 42 95 7F 7E 3D 69   
A2 BA A6 BE F3   
//固定   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00   
02 64 D2 0A 9D //固定   
00 10 //数据长度：16字节   
BA 5D 3D 29 C7 31 94 C9 52 18 84 83 60 9E 50 2E   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00   
03 //包尾   
]   
  
[NO.19 2012-03-16 20:04:19 799 RECEIVE 191字节]   
02 2B 27 00 30 2C D6 3B EB E4 1C 00 00 00 9F 3E   
36 D1 C8 AA 98 7B F9 75 0D 5B B9 4A B7 D3 F3 29   
8C 7A 52 DF 1B A2 83 1B F2 C4 8D C7 22 89 39 44   
A1 4A 75 2D 8E 99 8A DC 0E EB 91 44 95 80 E9 0A   
DA D3 47 E7 88 AF 17 D9 B9 5D 9C 01 26 C9 51 61   
C3 0E E2 3E A7 7F D9 1A 46 86 DE 1D D4 92 4C A8   
A1 F7 4E 05 0E 7F 3B 26 72 84 C5 90 ED 36 31 D0   
6E 06 67 A9 F5 67 A6 11 AA 0E F0 15 A4 72 07 7A   
12 80 FD FE B3 BE 5B 69 09 60 70 28 AB CC E2 7D   
55 8A 6D AF E1 6A E1 46 D5 FC A3 CF 05 60 60 2A   
79 C3 D3 E9 6F 78 41 6E AA 8C 0F 49 D3 81 5B 74   
BF 93 B3 17 48 C0 B3 92 BE 04 CE 0C 2F D7 03   
[   
02 //包头   
2B 27 //版本号   
00 30 //命令   
2C D6 //包序号   
3B EB E4 1C //QQ号码:1005315100   
00 //登录成功   
4E 66 6E 39 42 43 79 4A 50 76 55 63 42 64 7A 78 //Session Key   
3B EB E4 1C //QQ号码:1005315100   
72 F9 D6 6B //IP地址：114.249.214.107   
14 6B 4F 63 48 64 //未知   
00 00 00 00 //固定   
03 28 8F FE 4F BB B6 63 C7 69 C3 F1 3C DC A1 E8   
76 A3 CD 97 FA 00 26 00 74 08 00 00 00 00 00 00   
00 00 00 00 00 00 00 00 00 00   
08 02 //0030\_Token长度：2字节   
04 08   
08 08 08 08 04 05 01 F4 //未知8字节   
03 E8 07 D0 //固定4字节   
  
]

**qq消息包格式**

作者:　admin　　时间:　2012-06-10　　点击:　308次

\* \*\*\*\*\*\*\*\* 普通消息，消息类型为0x0009或者0x000A \*\*\*\*\*\*\*\*\*  
\* 头部  
\* --------- 加密开始（会话密钥）----------  
\* 发送者QQ号，4字节  
\* 接收者QQ号，4字节  
\* 包序号（并非我们发送时候的序号，因为这个是4字节，可能是服务器端得总序号）  
\* 发送者IP，如果是服务器转发的，那么ip就是服务器ip， 4字节  
\* 发送者端口，如果是服务器转发的，那么就是服务器的端口，2字节  
\* 消息类型，2字节，0x0009或者0x000A  
\* 发送者QQ版本，2字节  
\* 发送者的QQ号，4字节  
\* 接受者的QQ号，4字节  
\* md5处理的发送方的uid和session key，16字节  
\* 普通消息类型，比如是文本消息还是其他什么消息，2字节  
\* 会话ID，2字节，如果是一个操作需要发送多个包才能完成，则这个id必须一致  
\* 发送时间，4字节  
\* 发送者头像，2字节  
\* 是否有字体属性，4字节，有一般是0x00000001  
\* 消息的分片数，1字节  
\* 分片序号，1字节，从0开始  
\* 消息id，2字节，同一条消息的不同分片id相同  
\* 消息回复类型，这里的类型表示是正常回复还是自动回复之类的信息， 1字节  
\* 消息正文，长度 = 剩余字节数 - 包尾字体属性长度  
\* 字体属性，和SendIMPacket中的相同  
\* --------- 加密结束 ---------  
\* 尾部

**QQ协议分析**

作者:　admin　　时间:　2012-05-03　　点击:　297次

１、研究说明

　　Tencent在tqq.tencent.com的8000有一个使用HTTP的QQ接口，通过这个接口，可以进行一些基本的操作，如：登陆、登出、改变登陆状态(上线、忙碌、离线、隐身)、添加删除好友、查看好友信息、发送验证信息(接受被加为好友、申请加对方为好友、拒绝被加为好友)、收发用户消息、系统信息。

　　目前我研究的是1.1版本的HTTP QQ协议，研究是微程在的成果上进行的，不敢说有什么超越，只不过更为详细和准确。

２、接口说明：

　　接口位置：tqq.tencent.com:8000  
　　通信协议：HTTP  
　　数据传输方法：POST  
　　HTTP 请求格式：

POST HTTP/1.1  
Host: tqq.tencent.com:8000  
Content-Type: text/plain; charset=UTF-8  
Content-length: 长度  
Connection: close

数据

　　其中长度为 数据 的长度，数据的格式：  
　　VER=1.1&CMD=命令&SEQ=标记&UIN=QQ号& amp;....

　　以上４个参数是每个请求都必有的。其中，VER表示协议的版本，目前为1.1，据说1.2已经出来了，这个乱写的话，服务器返回NULL； CMD为操作的指令，有Login、List、Query\_Stat、GetInfo、AddToList、Ack\_AddToList、 DelFromList、Change\_Stat、GetMsgEx、CLTMSG、Logout；SEQ为当前请求的标记，防止重复发送，可以用当前时间，也可以用随机数；UIN是当前执行操作的QQ号。不过不同的CMD还需要不同的参数，下面我就公布我的研究成果。

３、研究方法：

　　我对目前网上的资料不够满意，就自己写程序，发送多条相同CMD不同参数的请求，根据服务器的返回，来做判断。感兴趣的朋友可以参考一下，此处可以跳过。  
　　下面我公布我探测的代码(PHP)：

$uin = "QQ号";  
$pwd = md5("QQ密码");

//登陆测试  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M5=1&LC=9326B87B234E7235";  
// 注意：登陆测试不能同时进行，必须等到服务器认为QQ断开了，才能够测试，不然结果不可信  
/\*\*\*\*\*\*\*  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M5=0&LC=9326B87B234E7235";  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M5=1&LC=9326B87B234E7235";  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M5=2&LC=9326B87B234E7235";  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M5=3&LC=9326B87B234E7235";  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M6=1&LC=9326B87B234E7235";  
$poststring[] = "VER=1.1&CMD=Login&SEQ=".rand(1000,9000)."&UIN=".$uin."&PS=".$pwd."&M6=1&LC=1223423545756679";  
\*\*\*\*\*\*\*/

//得到好友列表  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin;  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=160";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=160&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=160&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=".rand(1,200)."&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=".rand(1,200)."&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=".rand(1,200)."&UN=0";  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=List&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=106814";

//得到在线列表  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin;  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=160";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=160&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=160&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=".rand(1,200)."&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=".rand(1,200)."&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=".rand(1,200)."&UN=0";  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=".rand(1,10);  
$poststring[] = "VER=1.1&CMD=Query\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&TN=0&UN=106814";

//查看好友信息  
$poststring[] = "VER=1.1&CMD=GetInfo&SEQ=".rand(1000,9000)."&UIN=".$uin."&LV=0&UN=106814";  
$poststring[] = "VER=1.1&CMD=GetInfo&SEQ=".rand(1000,9000)."&UIN=".$uin."&LV=1&UN=106814";  
$poststring[] = "VER=1.1&CMD=GetInfo&SEQ=".rand(1000,9000)."&UIN=".$uin."&LV=2&UN=106814";  
$poststring[] = "VER=1.1&CMD=GetInfo&SEQ=".rand(1000,9000)."&UIN=".$uin."&LV=3&UN=106814";  
$poststring[] = "VER=1.1&CMD=GetInfo&SEQ=".rand(1000,9000)."&UIN=".$uin."&LV=4&UN=106814";  
$poststring[] = "VER=1.1&CMD=GetInfo&SEQ=".rand(1000,9000)."&UIN=".$uin."&LV=5&UN=106814";

//增加好友  
$poststring[] = "VER=1.1&CMD=AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814";

//发送验证  
$poststring[] = "VER=1.1&CMD=Ack\_AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&CD=0&RS=TEST";  
$poststring[] = "VER=1.1&CMD=Ack\_AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&CD=1&RS=TEST";  
$poststring[] = "VER=1.1&CMD=Ack\_AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&CD=2&RS=TEST";  
$poststring[] = "VER=1.1&CMD=Ack\_AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&CD=3&RS=TEST";  
$poststring[] = "VER=1.1&CMD=Ack\_AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&CD=4&RS=TEST";  
$poststring[] = "VER=1.1&CMD=Ack\_AddToList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&CD=5&RS=TEST";

//删除好友  
$poststring[] = "VER=1.1&CMD=DelFromList&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814";

//改变状态  
for($i=0;$i<=60;$i=$i+5)  
{  
$poststring[] = "VER=1.1&CMD=Change\_Stat&SEQ=".rand(1000,9000)."&UIN=".$uin."&ST=".$i;  
}

//获得消息  
$poststring[] = "VER=1.1&CMD=GetMsgEx&SEQ=".rand(1000,9000)."&UIN=".$uin."";

//发送消息  
$poststring[] = "VER=1.1&CMD=CLTMSG&SEQ=".rand(1000,9000)."&UIN=".$uin."&UN=106814&MG=TEST";

//登出  
$poststring[] = "VER=1.1&CMD=Logout&SEQ=".rand(1000,9000)."&UIN=".$uin."";

$file = fopen("p.txt","w");

foreach($poststring as $k=>$v)  
{  
ss\_timing\_start();  
$fp = fsockopen('tqq.tencent.com', '8000', $errno, $errstr, $timeout = 10);

if(!$fp){  
//error tell us  
$content = $k.chr(13).chr(10)."ERROR:$errstr ($errno)";

}else{

//send the server request  
fputs($fp, "POST HTTP/1.1\r\n");  
// fputs($fp, "Host: $host\r\n");  
// fputs($fp, "Content-type: application/x-www-form-urlencoded\r\n");  
fputs($fp, "Content-length: ".strlen($v)."\r\n");  
fputs($fp, "Connection: close\r\n\r\n");  
fputs($fp, $v . "\r\n\r\n");

//loop through the response from the server  
$res = "";  
while(!feof($fp)) {  
$res .= fgets($fp, 4096);  
}  
//close fp - we are done with it  
fclose($fp);

$content = $v.chr(13).chr(10).$res;  
}  
ss\_timing\_stop();  
$content .= chr(13).chr(10)."Time: ".ss\_timing\_current().chr(13).chr(10)."--------------------------------------".chr(13).chr(10);  
fputs($file,$content);  
}  
fclose($file);  
?>  
function ss\_timing\_start ($name = "default") {  
global $ss\_timing\_start\_times;  
$ss\_timing\_start\_times[$name] = explode(' ', microtime());  
}  
function ss\_timing\_stop ($name = "default") {  
global $ss\_timing\_stop\_times;  
$ss\_timing\_stop\_times[$name] = explode(' ', microtime());  
}  
function ss\_timing\_current ($name = "default") {  
global $ss\_timing\_start\_times, $ss\_timing\_stop\_times;  
if (!isset($ss\_timing\_start\_times[$name])) {  
return 0;  
}  
if (!isset($ss\_timing\_stop\_times[$name])) {  
$stop\_time = explode(' ', microtime());  
}  
else {  
$stop\_time = $ss\_timing\_stop\_times[$name];  
}  
$current = $stop\_time[1]-$ss\_timing\_start\_times[$name][1];  
$current += $stop\_time[0]-$ss\_timing\_start\_times[$name][0];  
return $current;  
}  
?>

４、研究成果：

(1).登陆  
　　说明：在你做任何其他操作以前，你必须登陆。只有在登陆以后，你的其他指令才有可能被正确执行(返回RES=0)，不然服务器会返回RES=20，不过有个例外，就是logout。当你成功登陆以后，服务器就会根据你的IP\*和参数中的UIN来验证身份。一台电脑可以同时登陆多个QQ，互不影响，就是因为有参数UIN。  
　　\*至于我能够确定服务器是通过IP来验证的，是因为服务器不可能通过我的请求获得其他信息了 ^\_^

　　提交数据：VER=1.1&CMD=Login&SEQ=标记&UIN=QQ号&PS=QQ密码& M5=1&LC=9326B87B234E7235  
　　说明：QQ密码是通过md5加密的字符串，在PHP中可以直接用md5()进行加密；  
　　　　　M5这个参数的作用还不清楚，但最好为1。  
　　　　　LC这个参数有点神秘，不能有丝毫改动，不然服务器就没有响应(没有响应就是返回NULL)。

　　返回：VER=1.1&CMD=LOGIN&SEQ=标记&UIN=QQ号&RES=0&RS=0& amp;HI=60&LI=300(成功)  
　　　　　VER=1.1&CMD=LOGIN&SEQ=标记& UIN=QQ号&RES=0&RS=1&RA=密码错误(密码错误)  
　　　　　VER=1.1& CMD=LOGIN&SEQ=标记&UIN=QQ号&RES=5(QQ号非法，如100)  
　　　　　NULL(UIN为字符、PS为空、LC错误)

(2).得到好友列表  
　　提交数据：VER=1.1&CMD=List&SEQ=标记&UIN=QQ号& TN=160&UN=0  
　　说明：TN、UN还不清楚具体表示什么，但是TN的值会影响返回的结果，有没有UN对结果没有影响

　　返回：VER=1.1&CMD=LIST&SEQ=标记&UIN=QQ号&RES=0&FN=9(当 TN=0或没有TN参数时，FN表示好友数)  
　　　　　VER=1.1&CMD=LIST&SEQ=标记&UIN=QQ 号&RES=0&FN=1& SN=9&UN=3814526,...,(当TN存在且非0时，FN=1，SN表示好友数，UN为好友列表，用","分割)  
　　　　　 VER=1.1&CMD=LIST&SEQ=标记&UIN=QQ号&RES=20(没有正确登陆)  
　　　　　 NULL(UIN、TN、UN为字符)

(3).得到在线好友列表  
　　提交数据：VER=1.1&CMD=Query\_Stat&SEQ=标记& UIN=QQ号&TN=50&UN=0  
　　说明：TN、UN还不清楚具体表示什么，但是TN的值会影响返回的结果，有没有UN对结果没有影响

　　返回：VER=1.1&CMD=QUERY\_STAT&SEQ=标记&UIN=QQ号&RES=0& FC=0,&FN=1&SN=1&ST=10,&UN=106814,&NK=Hackfan 好,(当TN存在且非0时，FN=1，SN表示在线好友数，FC、ST、UN、NK的值用','分割，分别表示头像、状态、号码、昵称)  
　　　　　VER=1.1&CMD=QUERY\_STAT&SEQ=标记&UIN=QQ号&RES=20(没有正确登陆)  
　　　　　NULL(UIN、TN、UN为字符)  
　　说明：FC为QQ头像的的ID，如的头像ID为270，那么其头使用的图片为91.bmp,其算法为ID/3+1；  
　　　　　ST为QQ用户的状态，10为上线，20为离线(或隐身)，30为忙碌；

　　特别说明：当参数TN=0或不存在时，服务器返回：

VER=1.1&CMD=Query\_Stat& amp;SEQ=标记&UIN=QQ号  
HTTP/1.1 200 OK  
Server: tencent imserver/1.0.0  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 56

VER=1.1&CMD=QUERY\_STAT&SEQ=标记&UIN=QQ号&RES=0&FN=1  
HTTP/1.1 200 OK  
Server: tencent imserver/1.0.0  
Content-Type: text/plain; charset=UTF-8  
Content-Length: 77

VER=1.1&CMD=QUERY\_STAT&SEQ=标记&UIN=QQ号&RES=0&FC=& amp;FN=1&SN=0&ST=&UN=&NK=

　　返回了２次，第一次的结果中，FN为在线好友数，第二次返回的数据基本没用。

(4).查看好友信息  
　　提交数据：VER=1.1&CMD=GetInfo&SEQ=标记&UIN=QQ号& amp;LV=查询类型&UN=被查询QQ号码  
　　说明：LV=0,1为精简查询，LV=2为普通查询，LV>=3为详细查询

　　返回：VER=1.1&CMD=GETINFO&SEQ=标记&UIN=QQ号&RES=0& LV=0&UN=106814&NK=Hackfan 好(精简查询)  
　　　　　VER=1.1& CMD=GETINFO&SEQ=标记&UIN=QQ号&RES=0&AD=地址&AG=19& EM=hackfan@qq.com&FC=0&HP=http://blog.hackfan.net&JB=学生  
& LV=2&PC=邮编&PH=电话&PR=The guy is updating to .NET Frameword......&PV=江苏&RN=胡吉阳&SC=毕业院校&SX=0&UN= 106814&NK=Hackfan  
好(普通查询)  
　　　　　VER=1.1&CMD=GETINFO& SEQ=标记&UIN=QQ号&RES=0&AD=地址&AG=19&BT=2&CO=6& CT=苏州&CV=%01&CY=中华人民共和国  
&EM=hackfan@qq.com&FC=0& HP=http://blog.hackfan.net&ID=-&JB=学生&LV=3& MO=136\*\*\*\*\*\*\*\*&MT=0&MV=&PC=邮编&PH=电话&PR=The guy is  
updating to .NET Frameword......&PV=江苏&RN=胡吉阳&SC=毕业院校&SH=3&SX=0& UN=106814&NK=Hackfan 好(详细查询)  
　　　　　VER=1.1&CMD=GETINFO& SEQ=标记&UIN=QQ号&RES=20(没有正确登陆)  
　　　　　NULL(UIN、LV、UN为字符)  
　　说明：AD为联系地址  
　　　　　AG为年龄  
　　　　　BT为血型  
　　　　　CO为星座  
　　　　　CT为城市  
　　　　　CV为未知\*  
　　　　　CY为国家  
　　　　　EM为Email  
　　　　　FC为头像  
　　　　　HP为网站  
　　　　　ID为未知  
　　　　　JB为职业  
　　　　　LV为查询代码(就是发送的LV)  
　　　　　MO为移动电话  
　　　　　MT为未知  
　　　　　MV为未知  
　　　　　PC为邮编  
　　　　　PH为联系电话  
　　　　　PR为简介  
　　　　　PV为省  
　　　　　RN为真实姓名  
　　　　　SC为毕业院校  
　　　　　SH为生肖  
　　　　　SX为性别  
　　　　　UN为QQ号  
　　　　　NK为昵称

　　　　　血型：0 => '',  
　　　　　　　　1 => 'A型',  
　　　　　　　　2 => 'B型',  
　　　　　　　　3 => 'O型',  
　　　　　　　　4 => 'AB型',  
　　　　　　　　5 => '其他'

　　　　　星座：0 => '',  
　　　　　　　　1 => '水瓶座',  
　　　　　　　　2 => '双鱼座',  
　　　　　　　　3 => '牡羊座',  
　　　　　　　　4 => '金牛座',  
　　　　　　　　5 => '双子座',  
　　　　　　　　6 => '巨蟹座',  
　　　　　　　　7 => '狮子座',  
　　　　　　　　8 => '处女座',  
　　　　　　　　9 => '天秤座',  
　　　　　　　　10 => '天蝎座',  
　　　　　　　　11 => '射手座',  
　　　　　　　　12 => '摩羯座'

　　　　　生肖：0 => '',  
　　　　　　　　1 => '鼠',  
　　　　　　　　2 => '牛',  
　　　　　　　　3 => '虎',  
　　　　　　　　4 => '兔',  
　　　　　　　　5 => '龙',  
　　　　　　　　6 => '蛇',  
　　　　　　　　7 => '马',  
　　　　　　　　8 => '羊',  
　　　　　　　　9 => '猴',  
　　　　　　　　10 => '鸡',  
　　　　　　　　11 => '狗',  
　　　　　　　　12 => '猪'

　　　　　性别：0 => '男',  
　　　　　　　　1 => '女'

(5).增加好友  
　　提交数据：VER=1.1&CMD=AddToList&SEQ=标记&UIN=QQ号& amp;UN=对方QQ号

　　返回：VER=1.1&CMD=AddToList&SEQ=标记&UIN=QQ号&RES=0& CD=0&UN=对方QQ号(允许被加为好友，此时他已经是你的好友)  
　　　　　VER=1.1&CMD=AddToList& amp;SEQ=标记&UIN=QQ号&RES=0&CD=1&UN=对方QQ号(需要验证)  
　　　　　 VER=1.1&CMD=AddToList&SEQ=标记&UIN=QQ号&RES=0&CD=2& UN=对方QQ号(决绝被加为好友)  
　　　　　VER=1.1&CMD=AddToList&SEQ=标记& UIN=QQ号&RES=20(没有正确登陆)  
　　　　　NULL(UIN、UN为字符)

(6).发送验证  
　　说明：1、如果你加对方为好友，你需要发送验证  
　　　　　2、对方加你为好友，发送了验证，你要通过或者拒绝  
　　　　　这2种情况需要发送验证消息

　　提交数据：VER=1.1&CMD=Ack\_AddToList&SEQ=标记&UIN=QQ号&UN=对方 QQ号&CD=验证类型&RS=理由  
　　说明：CD为0表示“通过验证”，CD为1表示“拒决加为对方为好友”，CD为2表示 “为请求对方加为好友”。

　　返回：VER=1.1&CMD=Ack\_AddToList&SEQ=标记&UIN=QQ号&RES=0(成功)  
　　　　　VER=1.1&CMD=Ack\_AddToList&SEQ=标记&UIN=QQ号& RES=3(\*)  
　　　　　VER=1.1&CMD=Ack\_AddToList&SEQ=标记&UIN=QQ号& amp;RES=20(没有正确登陆)  
　　　　　NULL(UIN、UN、CD为字符，RS为非UTF-8字符)  
　　\*如果服务器返回 RES=3，那么这次对话的响应时间在20s。当发送验证请求的时候，必须连发2次(请求内容不必一样)，其中一条RES=3，对方收不到，一条 RES=0，对方能够收到。当CD>=3时，RES=3，响应时间20s。

(7).删除好友  
　　提交数据：VER=1.1&CMD=DelFromList&SEQ=标记&UIN=QQ 号&UN=删除的QQ号

　　返回：VER=1.1&CMD=DelFromList&SEQ=标记&UIN=QQ号&RES=0& amp;(成功)  
　　　　　VER=1.1&CMD=DelFromList&SEQ=标记&UIN=QQ号& RES=3(响应时间30s，重复发送的后果)  
　　　　　VER=1.1&CMD=DelFromList&SEQ=标记& amp;UIN=QQ号&RES=20(没有正确登陆)  
　　　　　NULL(UIN、UN为字符)

(8).改变状态  
　　提交数据：VER=1.1&CMD=Change\_Stat&SEQ=标记&UIN=QQ 号&ST=状态代码  
　　说明：状态代码：10为上线，20为离线，30为忙碌，40为隐身，其他视为非法

　　返回：VER=1.1&CMD=Change\_Stat&SEQ=标记&UIN=QQ号&RES=0& amp;(成功)  
　　　　　VER=1.1&CMD=Change\_Stat&SEQ=标记&UIN=QQ号& RES=3(失败，原因不明，响应时间20s，可能是过于频繁的改变状态引起的)  
　　　　　VER=1.1& CMD=Change\_Stat&SEQ=标记&UIN=QQ号&RES=20(没有正确登陆)  
　　　　　 NULL(UIN为字符，ST非法)

　　特别说明：如果你改变好友，将会给所有好友发送一条系统信息，内容就是状态代码；如果隐身，发送的状态代码为20，表示离线。  
　　　　　　　同理，当你的好友改变状态，你也会收到一条系统信息。

(9).获得消息  
　　提交数据：VER=1.1&CMD=GetMsgEx&SEQ=标记&UIN=QQ号

　　返回：VER=1.1&CMD=GETMSGEX&SEQ=标记&UIN=QQ号&RES=0&MN =4&MT=99,99,99,9,&UN=36791785,99833581,99833581,106814,&MG=20,30,10,hi ,(MN表示信息数量，MT、UN、MG的值用","分割，分别表示消息类型、发送人号码、消息内容)  
　　　　　VER=1.1& CMD=GETMSGEX&SEQ=标记&UIN=QQ号&RES=0&MN=0&MT=&UN=& amp;MG=(表示没有信息)  
　　　　　VER=1.1&CMD=GETMSGEX&SEQ=标记&UIN=QQ号& amp;RES=20(没有正确登陆)  
　　　　　NULL(UIN为字符)  
　　说明：关于MT：  
　　　　　　　9为用户消息，99为系统消息，2为请求信息，3为通过验证，4为拒绝被加好友  
　　　　　关于MG：  
　　　　　　　当MT=9时，MG为用户发送的消息内容  
　　　　　　　当MT=99时,  
　　　　　　　　　MG=10(QQ\_STATUS\_ONLINE)表示对方上线  
　　　　　　　　　MG=20(QQ\_STATUS\_OFFLINE)表示对方下线  
　　　　　　　　　MG=30(QQ\_STATUS\_BUSY)表示对方进入忙碌状态  
　　　　　　　当MT=2时，MG为对方请求你验证的信息  
　　　　　　　当MT=3时，表示对方通过你的验证  
　　　　　　　当MT=4时，MG为对方拒绝你理由  
　　　　　　　当对方发送的消息过长时，服务器会自动截成几段，每段最多400个字节。完整的信息最后将有一个空格。  
　　　　　　　比如，我发送401个'A'的信息，接受的时候，服务器返回：  
VER =1.1&CMD=GETMSGEX&SEQ=标记&UIN=QQ号&RES=0&MN=2&MT= 9,9,&UN=106814,106814,&

MG=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA,A ,

　　　　　　　比如，我发送400个'A'的信息，接受的时候，服务器返回：  
VER=1.1&CMD=GETMSGEX&SEQ =标记&UIN=QQ号&RES=0&MN=2&MT=9,9,&UN=106814,106814, &

MG=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAA,A ,

　　　　　　　比如，我发送399个'A'的信息，接受的时候，服务器返回：  
VER=1.1&CMD=GETMSGEX&SEQ =标记&UIN=QQ号&RES=0&MN=1&MT=9,9,&UN=106814,&

MG= AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

AAAAAAAAAAAAAAAAAA ,

(10).发送消息  
　　提交数据：VER=1.1&CMD=CLTMSG&SEQ=标记&UIN=QQ号& amp;UN=对方QQ号&MG=发送内容  
　　说明：发送内容的长度应小于400字节

　　返回：VER=1.1&CMD=CLTMSG&SEQ=标记&UIN=QQ号&RES=0&(成功发送，对方不一定能收到哦)  
　　　　　VER=1.1&CMD=CLTMSG&SEQ=标记&UIN=QQ号& RES=3(发送过快或者内容超长>400个字节)  
　　　　　VER=1.1&CMD=CLTMSG&SEQ=标记& amp;UIN=QQ号&RES=20(没有正确登陆)  
　　　　　NULL(UIN、UN为字符，MG含非UTF-8字符)  
　　说明：1、当你发消息时，以下情形对方可能看不到(其实是收到了，QQ不提示)你发送的消息：  
　　　　　　　你俩互为陌生人，且对方没有和你说过话  
　　　　　　　你在他的陌生人列表里，并且他没有和你说过话(没有验证)  
　　　　　2、当你过快发送消息时，系统会给你一个惩罚，RES=3，相应时间20s  
　　　　　3、当我发送含有小写字母h的信息时，服务器有可能返回NULL  
　　　　　4、过长的消息需要分段发送，当消息长度超过400字节的时候，服务器返回RES=3

(11).登出  
　　提交数据：VER=1.1&CMD=Logout&SEQ=标记&UIN=QQ号

　　返回：VER=1.1&CMD=LOGOUT&SEQ=标记&UIN=QQ号&RES=0(成功，好像永远成功的，不管你是否登陆)  
　　　　　NULL(UIN为字符)

５、总结

　　通过对照以上的接口说明，我开发出了能够实现基本QQ功能的PHP类，它整合了以上所有的接口，使用更方便，可以开发QQ机器人、群发广告程序等。  
　　本文撰写时间仓促，难免有误，希望各位不吝赐教！