

**课 程 报 告**

**课程名称： 电子取证课程报告**

**专业班级： 信息安全201703**

**学 号： U201714513**

**姓 名： 徐立威**

**指导教师： 肖凌**

**报告日期： 2020年 5月 25 日**

**网络空间安全学院**

目录

[Windows中的QQ取证 1](#_Toc14728)

[1.1. 研究目的 1](#_Toc28680)

[1.2. 研究背景 1](#_Toc18165)

[1.3. 研究内容 1](#_Toc1431)

[1.4. 研究环境 1](#_Toc10084)

[1.5. 取证基本过程 2](#_Toc28944)

[1.5.1. 基本流程 2](#_Toc28227)

[1.5.2. 取证方法 2](#_Toc29110)

[1.5.2.1. 取证方法的版本差别 2](#_Toc6441)

[1.5.2.2. 方法途径 2](#_Toc25756)

[1.6. 版本差别研究 3](#_Toc30543)

[1.6.1. 早期08版本 3](#_Toc28865)

[1.6.2. 现在研究版本 4](#_Toc32188)

[1.7. 默认存储位置 5](#_Toc267)

[1.7.1. 账户及登录信息 5](#_Toc30155)

[1.7.2. 传输文件记录和文件内容 6](#_Toc25394)

[1.7.3. 聊天记录 6](#_Toc8443)

[1.7.4. 联系人、群组相关信息 7](#_Toc23249)

[1.8. 文件存储位置研究 8](#_Toc1066)

[1.8.1. 存储位置 8](#_Toc12860)

[1.8.2. 位置修改 10](#_Toc23971)

[1.8.2.1. 接收文件位置 10](#_Toc24266)

[1.8.2.2. 文件夹存储位置 11](#_Toc9387)

[1.8.2.3. 图像视频位置 12](#_Toc15545)

[1.9. 图像存储 13](#_Toc9841)

[1.9.1. QQ群下载的图像 13](#_Toc18127)

[1.9.2. “我的手机”下载的图像 14](#_Toc13203)

[1.9.3. 发送截图照片存储 14](#_Toc4196)

[1.10. 消息管理器 16](#_Toc10888)

[1.10.1. 基本介绍 16](#_Toc15494)

[1.10.2. 基本操作 16](#_Toc20153)

[1.11. 聊天内容的解析 19](#_Toc17224)

[1.11.1. 定位 MsgEx.db 中有效数据 19](#_Toc6419)

[1.11.2. 数据的解密分析 19](#_Toc7806)

[1.11.3. 信息存储结构 20](#_Toc22088)

[1.11.4. 新版QQ聊天内容解析 20](#_Toc376)

[1.12. 其他取证信息 20](#_Toc18475)

[1.13. 联系运营商 21](#_Toc7035)

[1.13.1. 公安调用QQ信息 21](#_Toc27329)

[1.13.2. 法律依据 21](#_Toc8961)

[1.14. 研究小结 23](#_Toc17147)

# Windows中的QQ取证

## 研究目的

电子取证是指利用计算机软硬件技术，以符合法律规范的方式对计算机入侵、破坏、欺诈、攻击等犯罪行为进行证据获取、保存、分析和出示的过程。QQ作为目前最为流行的聊天工具之一，在网上交互担当着重要的角色，其账户信息也与许多的其他平台有着绑定关系.因此QQ是取证信息的重要来源，很多的证据都能从QQ中获取，研究QQ取证具有着重要意义。

## 研究背景

随着网络逐步进入我们的工作和生活，人们对信息实时性的要求越来越高，与外界的联系，也不再仅仅局限于电子邮件和电话，而是需要网络信息的实时传递。

QQ 是腾讯公司 1999 年推出的即时通信软件，目前也是国内最流行的聊天工具之一。 其不仅能传递文字消息，还集成了文件传输、语音聊天、视频会议、电子邮件、用户群、新闻浏览、短信发送、微博等诸多功能。 越来越多的用户通过 QQ 软件进行语音视频聊天、资源共享、发送电子邮件或者组建用户群。

随着 QQ 的广泛应用， 利用 QQ 软件进行恶性犯罪的案例也成逐年上升趋势。 如发布虚假中奖信息及钓鱼网站，侵犯他人财产安全；联络、煽动组织成员进行打砸抢烧，危害公共安全；泄露国家秘密、情报或军事秘密，危害国家安全等。 自 2005 年以来，随着国家司法鉴定制度的逐步推进，QQ 取证及其司法鉴定是打击此类犯罪活动的主动手段，是震慑此类犯罪活动国家意志的具体体现。 因此，开展 QQ 取证与司法鉴定方法研究具有迫切的现实意义。

## 研究内容

主要研究的内容包括：账户及登录信息；传输文件记录及文件内容；聊天记录；联系人、群组相关信息等，个人会从存储位置、文件功能、取证途径等各种角度出发，研究在取证过程中的重要证据的获取方式。

## 研究环境

操作系统：windows 10

QQ版本：QQ 9.3.3

内存大小：8G

## 取证基本过程

### 基本流程

* 录像。取硬盘、具体的实施操作过程录像，屏幕也录下像（用软件），这样使的取证过程更具有说服力。
* 镜像备份。硬盘拿下来之后，可以先进行一次复制，或者制作镜像。然后对硬盘进行HASH值计算。（如果做了复制，或者镜像，那么就用复制的盘进行操作）
* 编号。给机器和硬盘编号、拍照。
* 记录。最好有一个完整的记录链，用来说明检材的状态、存放位置始终处于可控状态。操作现场也可以有个记录，或者有个报告，说明当时的环境，以及取证的计算机的一些设备、配置、系统等。
* 取证。使用取证软件（如SA、取证大师等）对检材硬盘进行即时通信分析。

### 取证方法

#### 取证方法的版本差别

* 如果是QQ2008或更早版本，可以直接分析出来。里面的信息按文件分别存储，没有加密处理。这个时候的版本可以直接查看取证对象的信息，十分的简单，之后也会进行简单的介绍。
* 如果是QQ2009或更新版本，则先要在本地（也就是进行取证的机器上）登录要解析的QQ账号。然后在SA即时通信分析窗口中勾选在弹出的窗口中选择要解析的QQ号（也就是已经在本地机器上已经登录了的），获取KEY。获取成功后，就可以分析出该账号所有的聊天记录，包括被删除的。

#### 方法途径

* QQ大致的加密原理：QQ对密码和聊天内容的保存，都不是明文的，是进行过加密的。在登录的时候，我们输入的会密码进行2次MD5运算，之后，发送到腾讯的服务器上，再生成一个KEY。这个KEY会发回给本地的QQ，用这个KEY进行登录的验证以及对聊天内容的解码。
* 通过了解加密原理，可以知道，QQ聊天记录的解析，关键在于得到这个KEY。为了得到这个KEY，我们就需要成功登录上QQ，然后将腾讯服务器上的发回来的KEY截获，这样就可以解析该QQ号中所有的聊天记录了。
* QQ将聊天记录，保存在安装目录下的“msg3.0.db”文件中。如果我们将检材硬盘接在只读接口上，那么，检材中的“msg3.0.db”是不会被修改的。而我们的SA虽然需要通过在本地登录上该QQ账号来获取KEY。但最终解析的是检材中的“msg.3.0.db”文件。所以，是不会出现证据遭到破坏的问题。这样就能保证证据的合法性、完整性、原始性。

## 版本差别研究

### 早期08版本

这个版本的QQ还处于初步发展的过程，其性能要求远高于安全需求，当时的目标也就是能实现用户之前的互相交流就行，所以在信息安全上不重视，很多的聊天信息都是明文传输，QQ好友等信息也可以进行随便的转移。

就拿联系人信息举个例子，当时如果丢号了，想要加回之前的好友，那么只需要把电脑中User.db 复制到新QQ的目录下即可。这样新QQ就会有之前QQ的好友名单。但是这种情况并不能直接和对方通话，还是需要好友认证的过程，这些好友只是镜像。因此，这种情况下的QQ很容易泄露个人隐私，比如在网吧等公众场所，如果没有及时的关闭电脑，或者电脑也没有对信息进行清理。那么即使你关闭了QQ，对方也很容易的拿到你好友的信息，这是相当危险的。

同样的，也因为安全措施做得简陋，对于早期的QQ版本可以直接复制文件信息取证。下面是有关早期QQ各个文件的功能：

默认安装QQ的位置:

C\Program Files\Tencent\QQ\XXXX

用户文件：

Config.db QQ 系统设置

Content\_Config.ini 自定义面度板设置

ewh.db QQ 密码

MsgEx.db QQ 聊天记录

notes.db QQ 备忘录

QQMailSettingEx.dat QQMail 设置

QQMailAddr.dat QQMail 地址本

QQMailIndex.dat QQMail信息

QRT.dat QQ 炫铃信息

MailData QQMail 本地邮件

ShareInfo.db 共享属文件夹设置

User.db QQ本地好友列表

VQQ.db QQ 视频设置

QQAVFile 好友QQ秀缓存目录

CustomFace QQ 自定义表情目录

CustomFaceRecv 接收的 QQ 自定义表情保存目录

### 现在研究版本

现在的QQ版本有了很大的改动，因此在取证方法上也有了很大的差别，不能直接从文件中获取信息，需要借助取证工具对QQ账号进行解析。我将对比前后版本文件的更改，来观察修改了哪些部分，观察的文件主要是.db、.dat格式。

从图1和图2中可以看到.dat文件只有一个，.db文件类型也大有改变。目前发现唯一没有较大改动的只有Msg文件，也就是QQ聊天记录，但是据了解，里面的信息不再是明文存放使用了。

其他的文件存储信息，例如：

Info.db 个人形象的信息

Infocenter.db 迷你首面

Misc.db 自定义头像

Registry.db 自定义图像/好友列表

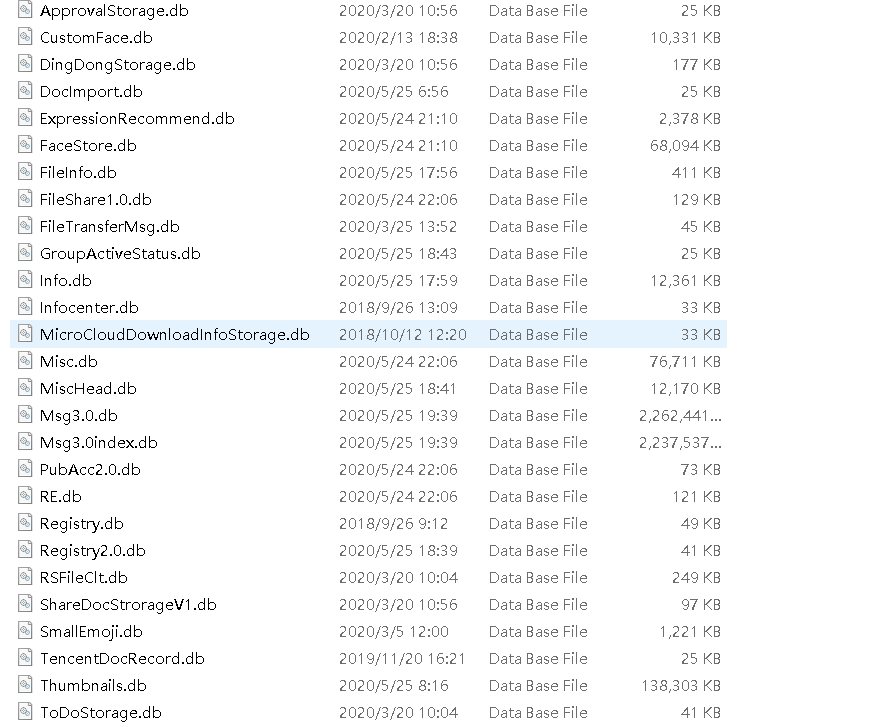


图1 .db文件



图2 .dat文件

再加上文件信息进行了加密处理，即使拿到了.db文件，进行破解也是较大的工程。但是根据我的了解，在中国基本上司法机关如果想要获得QQ聊天记录的话是可以直接向腾讯公司进行申请的，所以在获得取证对象的QQ账号后，事情就变得相对容易的多。

## 默认存储位置

### 账户及登录信息

账户及登录信息一般位于安装的QQ目录下，可以在QQ快捷方式点击打开文件所在位置，可以直接到QQ目录下的bin文件，返回父目录即可，如图3。以前的版本可以找到User文件夹，双击该文件就可以获得之前所有登录过的账号，如图4。如图5，我们可以看到现在的版本将User文件夹删除了，有了一定的改动，但估计用户信息依旧存储在这里。

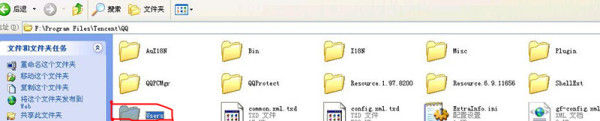


图3

IMG_256

图4

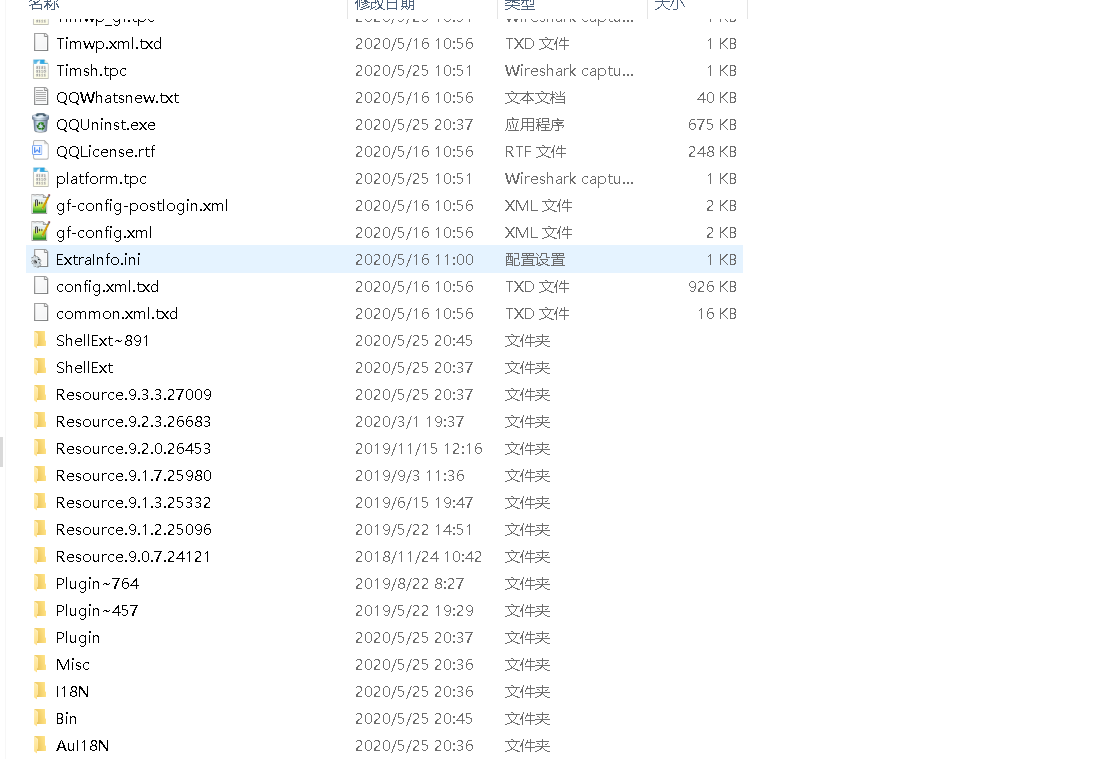


图5

### 传输文件记录和文件内容

在前面也有所介绍，通常的来说传输文件的下载位置是可以更改的，每个用户都可以更改成不同的位置，彼此之间互不干扰。所以个人有这样的想法，可能存在这种情况，有个人恶意的把自己的文件下载地址修改成和他人的下载地址一样，然后再把文件下载地址改回默认的来冒充另外一个人下载过这个文件。

但是，如果用户第一次在该电脑登录的话，一般都是默认地址C:\Users\Administrator\Documents\Tencent Files\xxxxxxxxx\FileRecv。如图6所示。

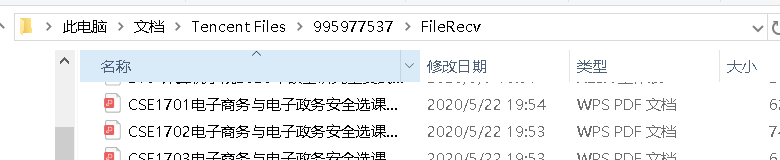


图6

### 聊天记录

如图7，C:\我的文档\Tencent Files\xxxxxxx里面的一个名称为“Msg3.0.db”文件，我的文件大小有2G（聊天信息有点多）。这里存放的是用户的聊天记录，后面的3.0是版本，之前流行的是2.0版本。

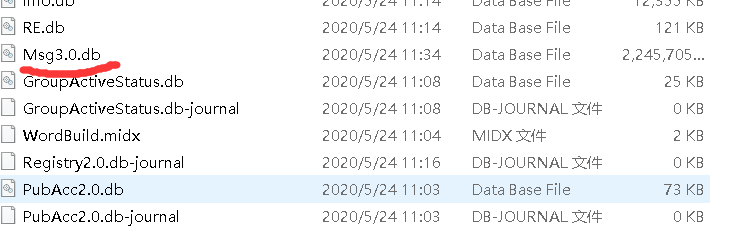


图7

但是如果想查看具体的内容，需要登录QQ才能查看。Msg.db是聊天记录的数据文件，Message.cfg是消息配置文件，而User.db则是用户信息数据库文件。很多人重装QQ都会保制存这三个文件，再复制到新装的QQ的文件里，但是现在的版本基本上没有了

所以电子取证的时候，这个文件至关重要，但是要获取里面的信息还是先破解用户密码，然后将该文件放到相应位置，来查看用户与其他人的聊天记录。同样的如果换电脑的时候想把一台电脑之前的信息也传输过去，具体的操作也是对该文件进行复制粘贴。

然后还发现，文件当中有几个-journal的后缀，这是漫游文件夹的特征，主要是方便用户在切换电脑的时候还能存有之前的信息而设置的。这个文件夹是从云端下载下来，体积不能过大，所以一般设置为7天漫游，只能存储7天内的信息。

想要打开这些文件，个人推荐可以采用QQ内置的消息管理器，只要把文件或文件夹导入进去，就能看到里面的聊天信息，不过不支持其他账号登陆本账号，这可能需要得到QQ的技术支持才能实现。

### 联系人、群组相关信息

早之前的版本联系人存储在User.db当中，但是现在该文件已经没有，取而代之的是Registry.db。Registry.db是自定义图像/好友列表的数据存储位置，为了查找我搜索下Registry。从中我可以找到9个文件，如图8。然后找了各自对应的地址，如下所示：

C:\Users\Administrator\Documents\Tencent Files\QQ号码\QQ

C:\Users\Administrator\Documents\Tencent Files\QQ号码\TIM

C:\Users\Administrator\Documents\Tencent Files\QQ号码

每个地址都有Registry.db、Registry2.0.db、Registry2.0.db-journal三种文件，而我们也可以看到上面的三个地址真好就是QQ、TIM以及它们的父地址，这也解释QQ和TIM不能同时登陆的原因，它们都是使用同一个文件夹，信息之间也是共享的。利用这个特点，有时候可以从TIM方向入手。这三个文件名中，2.0代表着版本号，-journal是漫游，我没开启漫游因此大小都是0 KB。

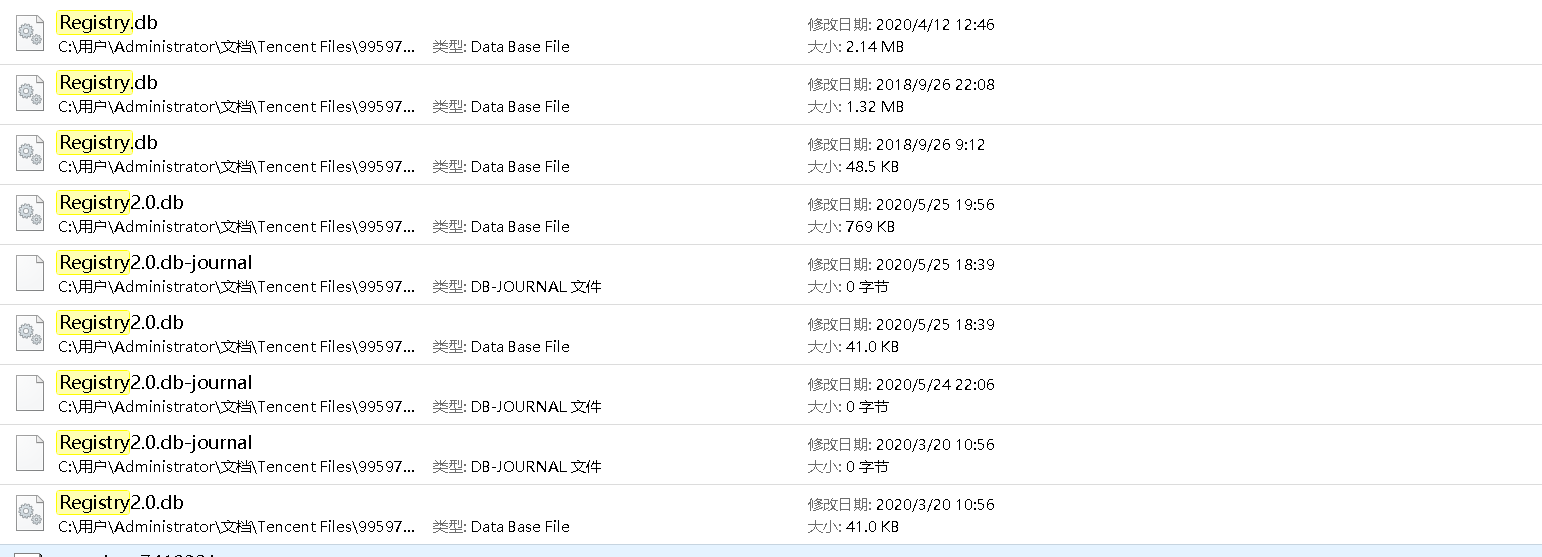


图8

## 文件存储位置研究

### 存储位置

QQ文件存储位置并不是固定不变的，它是可以由用户进行修改。但一般默认的存储地址是再我的文档的Tencent Files文件当中。因此在取证过程中，需要正确的判断取证对象的QQ是否是默认存储，如果不是默认存储就还需要进一步的判断。

点击左下角的主菜单，会有退出、切换账号、关于QQ、设置等栏目，如图9所示。在这些功能里，打开设置，里面有文件管理，文件管理的界面如图10所示。

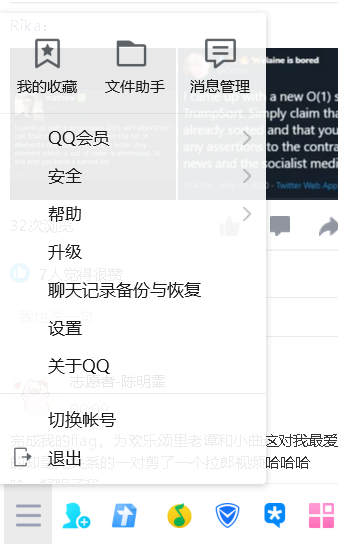


图9 QQ主菜单

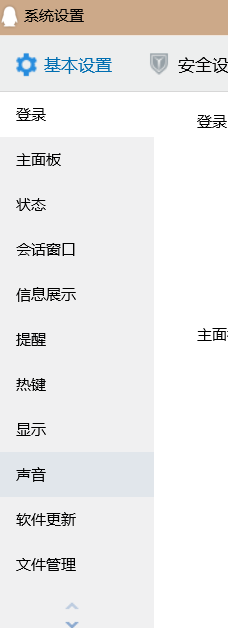


图10

如图11，在基本设置下点击文件管理就会定位到默认文件存储位置，显然我的文件存储地址是默认格式，如：C:\Users\Administrator\Documents\Tencent Files\xxxxxxxxx\FileRecv\。



图11

再往下滑，可以看到音视频通话，这里是视频存储的位置，也是一个默认文件地址...\QQ\Photo，如图12。



图12

### 位置修改

#### 接收文件位置

如图13，在点击完文件管理后，第一个修改就是下载文件位置的修改。FileRecv这个文件夹一般是存储QQ聊天时下载的文件，修改只需要更改目录即可。如果改成其他的目录下载，是不会对前面下载的文件进行搬移。



图13

然后，个人做了下实验，假设先下载一个文件，然后修改接收文件存储位置后再下载一个文件。发现之前下载的文件依旧定位到之前的文件夹，而第二个下载的文件则是定位到修改后的文件夹位置，如图14。而且文件下载还可以进行另存为操作，所以我觉得必须要有足够的证据来证明下载文件是从取证QQ中下载的，否则缺少可信度，这个问题可能是很多软件共同面临的问题，所以暂时不再深究。

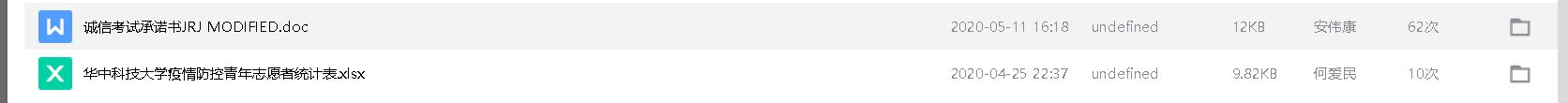


图14 下载的两个文件

#### 文件夹存储位置

在接收文件位置的下面就是文件夹存储位置的修改，我将选择个人文件夹的保存位置改成自定义。如图15所示：

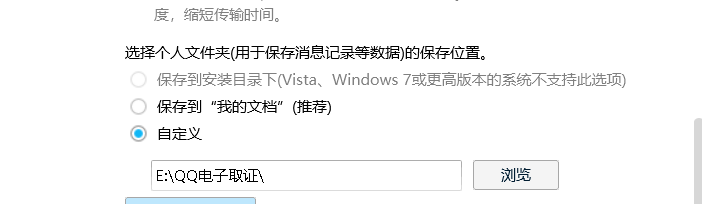


图15

当时我以为只是新建一个文件夹，后面发现QQ会进行文件迁移操作，如图16。如图17，我的文档中的文件会被迁移到修改后的地址当中。当然也可以选择跳过，终止迁移，但是这样做的话，QQ可能就会找不到之前的聊天信息，如图18。如图19，迁移过程中间卡住了，我就直接取消了，看下迁移后的结果。

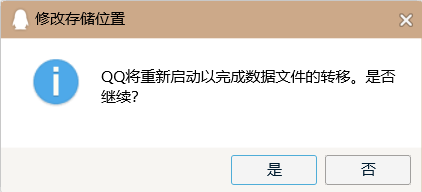


图16 数据文件迁移

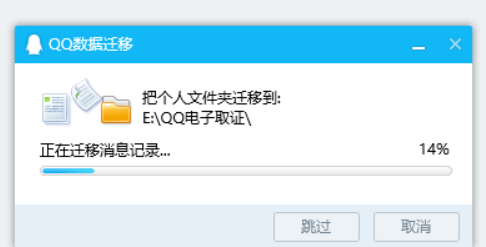


图17 数据迁移加载图

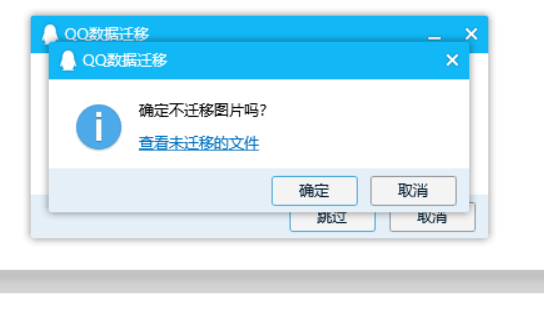


图18 终止迁移

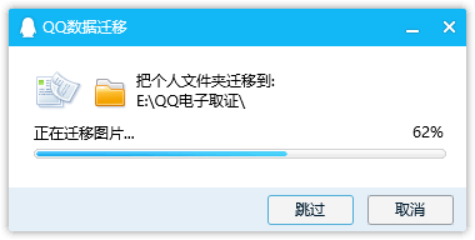


图19 迁移卡住

#### 图像视频位置

如图20，往下滑到底是拍照所得照片的存储位置，在Photo文件当中。但是后面发现，在QQ聊天时候看到的图片并不是存储在这个位置，这个可能只是直播视频截图的位置。而QQ聊天的图片是存储在另外一个位置，这个我将在后面进行详细的分析。



图20 图像视频

## 图像存储

### QQ群下载的图像

这是我从QQ群下载的文件，打开文件所在位置找到的文件夹，发现是在...\QQ账号\image文件夹当中，图片的名字具有一定的特点，下面将对其进行分析。

在图21中可以看到，图片的名字是：2@S)E[U4M0O18(MOW\_{2EIX.bmp。对应图像所在位置，不难发现，其中的2@S)是前面两层的文件夹的名字:\2@\S)，因此可以简单的从名字命名来判断图片的所在位置。

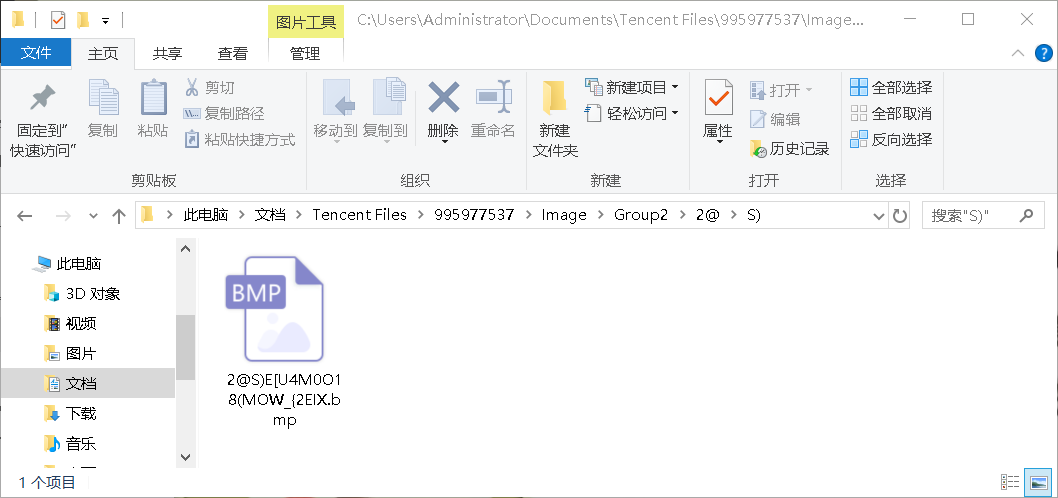


图21 图像存储位置

翻阅前面两个文件目录，可以发现都是文件夹名都是由两个字母符号组成如图22。且如果文件名的第一个符号相同，其文件的修改日期就会相近，几乎同时修改，如图23。但是我观察了下两张同时发出的图像，他们并不是在相邻的文件夹，存在着一定的时差。所以个人的猜测是，这些文件夹会根据它命名的顺序进行规律的批量的处理（比如杀毒、转移图像这类需要访问文件的操作），这很符合代码的循环操作。

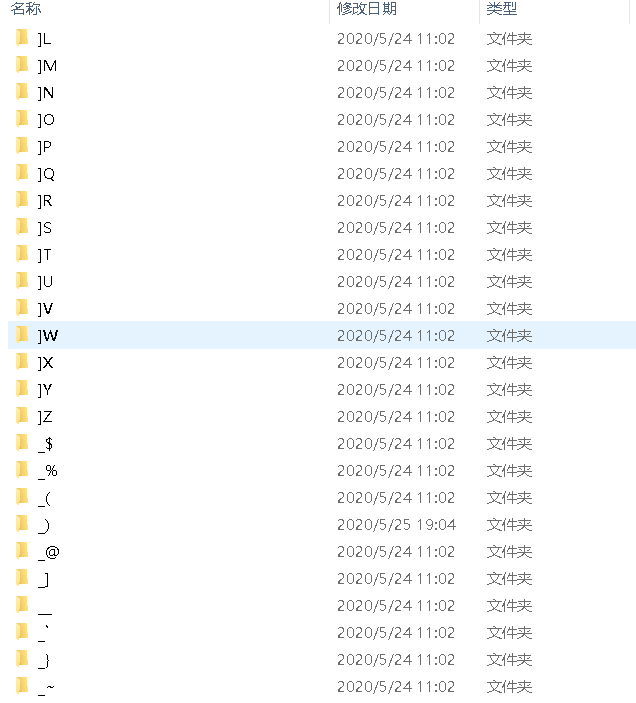


图22 前两个目录

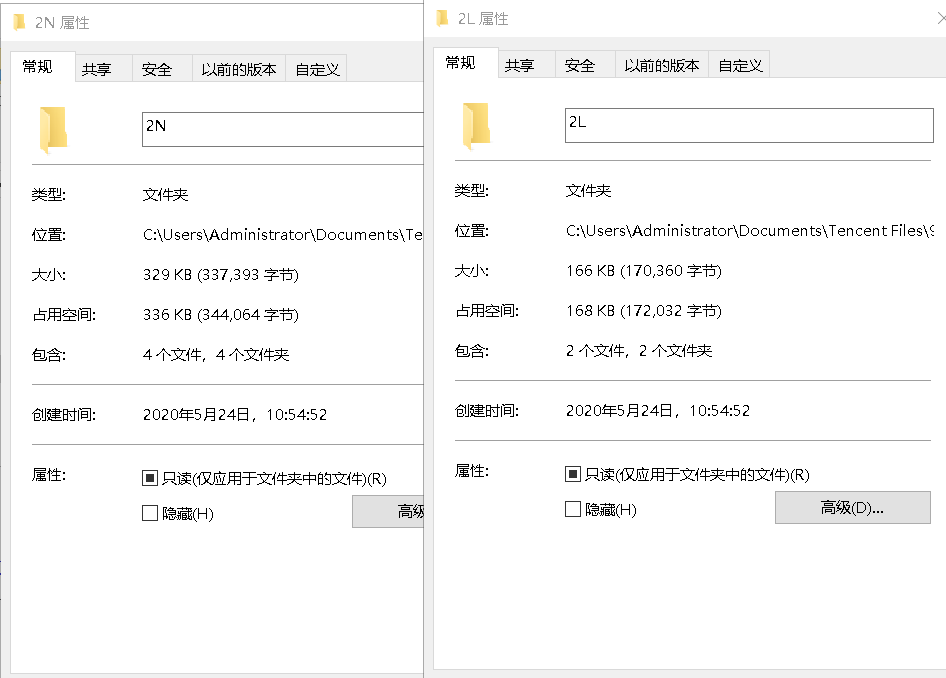


图23 两相“近”文件对比

### “我的手机”下载的图像

如果是我的手机上传到我的电脑当中，和前面的情况有所不同，位置也不是之前所说的\image文件夹当中。如图24，默认位置在

C:\Users\Administrator\Documents\Tencent Files\xxxxxxxx\FileRecv\MobileFile。

这个命名也十分的好理解，MobileFile翻译下是手机文件。令人感到好奇的是，在这个目录当中，还有一个image文件夹，这个文件夹是做什么用的呢？

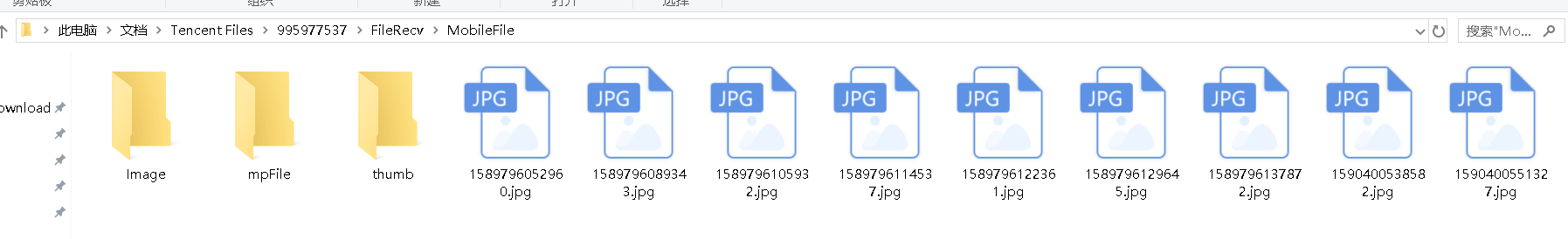


图24 手机存储地址

打开image文件夹中的图片，发现里面是我发给手机的图片，而且是截图照片，说明这个文件夹会存储QQ截图发送给手机所留下的照片。如果是已有的照片发送给我的手机，是不会有所谓的“副本”在该文件当中，这个我也已经做过实验证明。

### 发送截图照片存储

我尝试截图发送，发现发送对象不同也会有不同的结果。主要来说我探究了3个对象，QQ群、QQ好友、自己（我的手机）。

我的手机已经前面分析了，它会存储到...\QQ号码\FileRecv\MobileFile\image中；QQ群主动截图会先存储到...\QQ号码\QQ\WinTemp\RichOle当中，这是个临时文件，后面文件将还是存储至\QQ号码\Image\Group2当中；发送给QQ好友的截图可以在...\QQ号码\Image\C2C。

对于...\QQ号码\QQ\WinTemp\RichOle，网上并没有过多的描述，但是可以猜测这是windows系统下的QQ临时存储的位置。而c2c文件夹是存储qq聊天记录的图片,主要是你截图发送给QQ好友的照片，但是在网上有些人说是别人发过来的照片，我感觉这个需要纠正。

下面是实验图片：

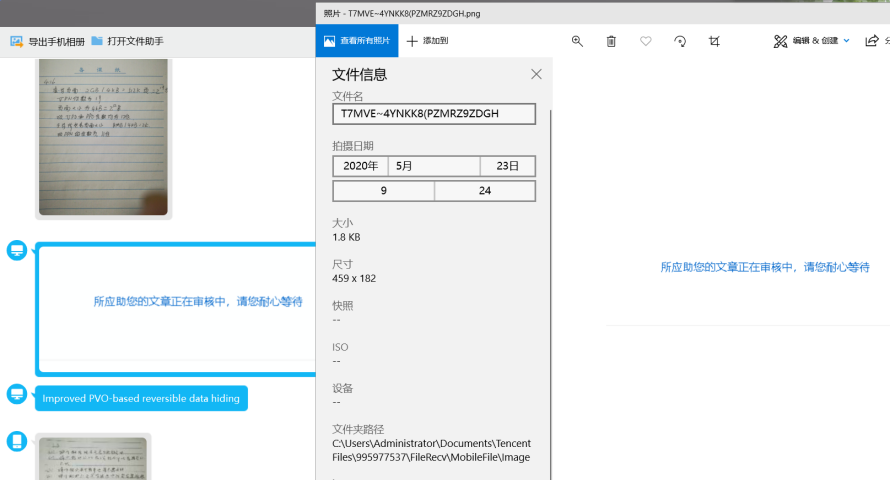


图25 发送手机截屏

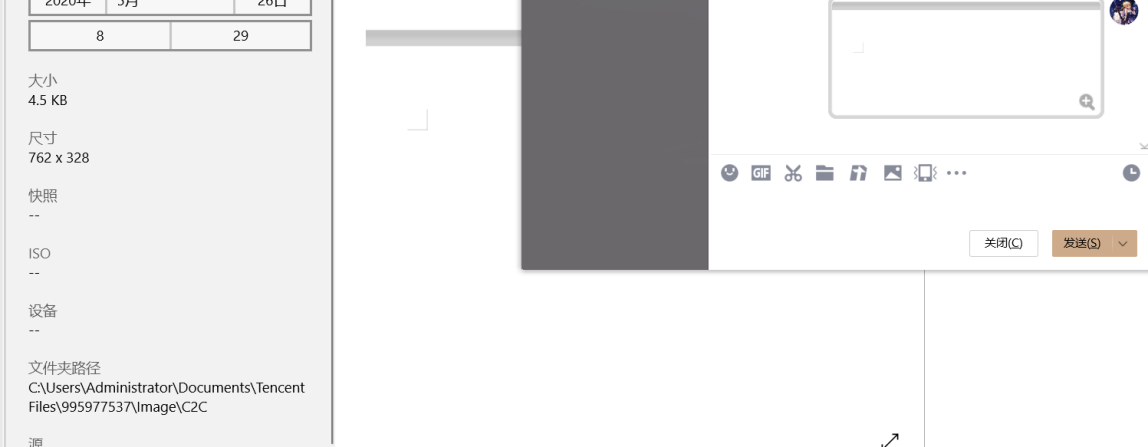


图26 发送好友截屏

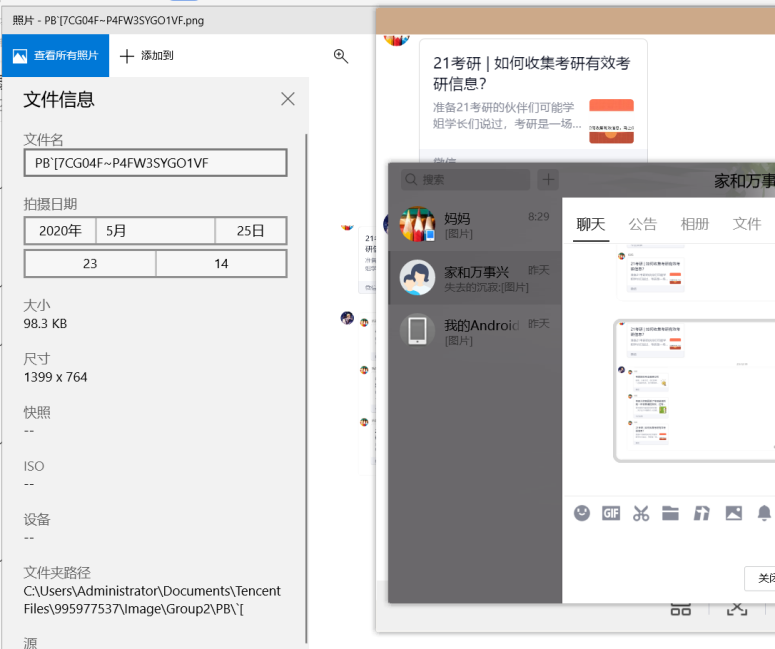


图27 发送QQ群截图

整理下，方便浏览：

* 手机发送截图：

..\QQ号码\FileRecv\MobileFile\image

* QQ群发送截图：

...\QQ号码\QQ\WinTemp\RichOle

...\QQ号码\Image\Group2

* QQ好友发送截图：

...\QQ号码\Image\C2C。

## 消息管理器

### 基本介绍

QQ的消息管理器是对用户信息的处理器，具有着信息导入导出等功能，如果用户丢失了之前的历史信息，或者想把之前电脑的历史信息转移到新电脑当中都可以用消息管理器进行操作。

### 基本操作

#### 打开消息管理器

消息管理器在9.3.3版本稍微放的隐蔽，之前版本可以直接在主菜单上找到，在新版本QQ需要打开设置，在安全设置点击消息记录，如图28。可以看到消息记录这里有打开消息管理器的按键。打开之后就如图29所示。



图28



图29

#### 导入消息

在消息管理器的右上角，有个倒三角形，点击这个符号导入信息、导出全部信息、云消息设置三个功能。

我们先来看下导入信息功能，这个功能有3种导入方式，自动搜索、从指定目录导入、从指定文件导入，如图30。

自动搜索导入是按照默认文件夹进行导入，这十分的适合重新安装QQ后发现之前信息全部消失的情况。

从指定目录导入，则是把...\Tencent Files\QQ号码文件夹导入进来。

从指定文件导入，则是导入.db和.bak文件，也就是历史消息的存储文件。

我曾今尝试过利用我的账号导入其他人的消息记录，可能存在认证匹配的问题，出现闪退。所以个人认为还是获得原账号的QQ最好，或者有专门的QQ取证工具能对信息进行解密。

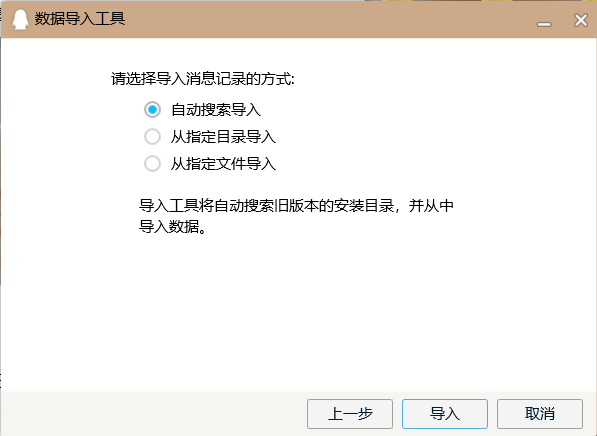


图30

#### 导出消息

导出信息同样有三种方式，加密文件、网页格式、文本文件，如图31。

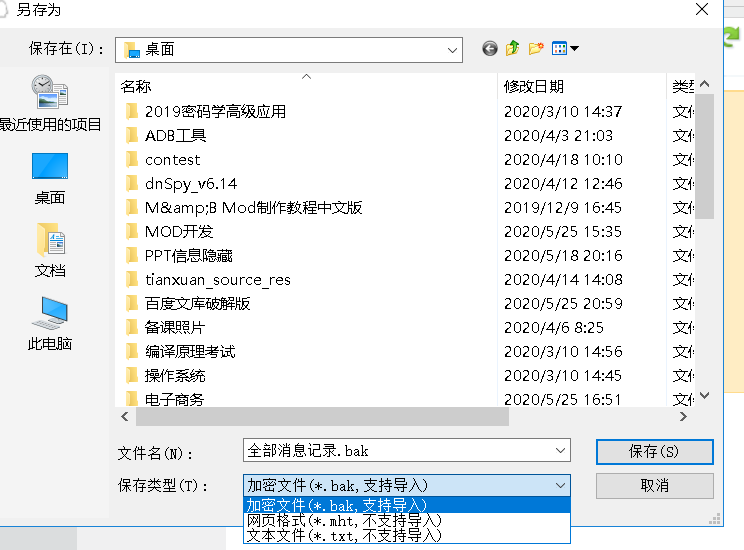


图31

加密文件：导出后的文件夹名字为全部消息记录.bak，具有一定的加密保护，如图32。导出的文件不能直接打开，需要消息管理器或者取证工具进行打开。而且我也尝试了一下，如果导出的消息记录较小还好，一旦很大，貌似总是在加载一半的时候就会闪退，然后在导出位置也找不到相应的导出文件，这个也可能是个人电脑自己的问题。

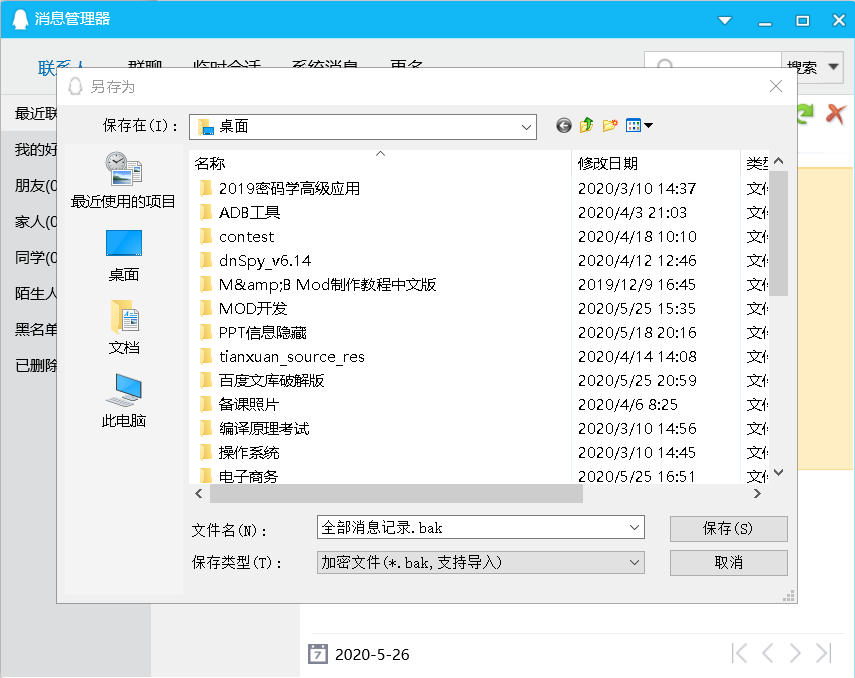


图32

网页格式：导出的文件格式是.mht，可以直接的打开，而且里面会有详细的信息，如消息分组、对象、日期、内容等，如图33。

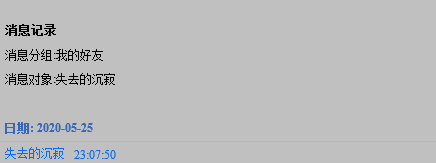


图33

文本格式：与网页格式类似，但是因为表现形式的局限性，文本模式是不能导出图片的。

## 聊天内容的解析

### 定位 MsgEx.db 中有效数据

这个是早期版本QQ的解析，对现在版本的QQ有一定的参考价值。

聊天内容的数据是存储在 MsgEx.db 根仓库下的名称为 C2CMsg、SysMsg、DiscMsg、GroupMsg、MobileMsg、TempSessionMsg 仓库下，分别代表着好友消息、系统信息、多人聊天消息、群组消息、移动 QQ 消息、临时会话消息并且每个仓库下分别有 Data.msj 和 Index.msj 两个流。其中，聊天记录内容存放在 Data.msj 中，Index.msj 为一个索引文件，具体消息内容已经经过加密。

另外，Matrix 仓库下的 Matrix.db 流，在解密的过程中也要用到。

### 数据的解密分析

消息内容采用 BlowFish 分组加密。破解步骤如下：

1）生成 BlowFish 的全局公用密钥 Key，Key 要通过 QQ 号码生成，具体步骤是：

(ⅰ)将 QQ 号码进行 MD5 变换，得到 Md5Key；

(ⅱ)取 Matrix.db 的数据，对其进行解码。

简单介绍一下 Matrix.db文件的结构： Matrix.db 采用分块存储，每个 Record 包含类型、名字长度、名字、内容长度、内容几个字段组成。其内容也是通过加密存储的。

解密方法是：

将长度的低位字节和高位字节 XOR，得到 key；将内容逐个与 key 进行 XOR，就得到结果。对名字和内容分别进行解密即可。解密后会看到 STL、 TIP、 CRK、 CPH、CAH 等字段。我们要用到的是 CRK 字段，长度为 32 字节。将得到的 CRK 字段作为 pData；

(ⅲ)用 Md5Key 对 pData 进行 BlowFish 解密，得到全局密钥 Key。

2）BlowFish 算法解密，每 8 个字节为一个分组。密钥 Key 在第 1）步中生成。解密的方法是：

(ⅰ)取前 8 个字节，通过 BlowFish 解密， 得到 decryptKey；

(ⅱ)decryptKey 与后面 8 个字节 XOR，对结果再进行一次 BlowFish 解密；

(ⅲ)将 decryptKey 与前 8 个字节 XOR，得到第一组结果；

(ⅳ)decryptKey 与后面 8 个字节 XOR，重复(ⅱ) (ⅲ)两步；

(ⅴ)最终全部数据解密完毕。最后会剩下一组 8 字节无法解密，实际上这个是没有用到的数据，可能是用来作为校验的。

### 信息存储结构

根据前面的解析过程，基本可以解析出具体的聊天内容信息，但是在解析过程中，还要加进消息归类的步骤，将内容具体归为好友消息、群组消息、临时会话消息等等

### 新版QQ聊天内容解析

新版 QQ 在没有登陆口令的情况下想要获取本地聊天记录信息目前还很困难，但并不意味着我们针对 QQ 取证的工作不能进行。 根据具体情况，以下三条思路值得我们进一步研究：

一是针对 QQ2009sp5之前的 Msg2.0.db 文件，可以采取替换 info.dat 和 Matrix.dat 结构中的部分关键二进制信息来打开文件，读取聊天记录，实践证明这个方法是可行的。

二是根据用户登录网站、论坛、邮箱的密码推断 QQ 密码。 据统计，人们通常使用的密码数量有限，一般不会超过 6 个，可以通过查看注册表等方式找出相应密码来推断QQ 密码。 在鉴定过程中应避开原始检材而在取证计算机上重建该 QQ 号码的原有环境，并针对提取过程采取屏幕录像等手段以确保检材的原始性。

三是通过嫌疑人手机 QQ 获取登陆口令， 进而用于计算机中QQ 客服端聊天记录获取。 笔者在研究手机取证时发现，手机上网用户在使用手机 QQ 的过程中喜欢保存登陆口令以便随时登陆，而多数手机系统平台对保存QQ 登陆口令的安全性重视不够， 这样在有必要的情况下，可以将手机取证与 QQ 取证结合起来，获取 QQ聊天记录信息。

## 其他取证信息

QQ 是一款即时聊天软件，对其取证，重点应放在对聊天记录的获取上，因为聊天记录包含的证据信息量多，且可以反映嫌疑人网络通信脉络及过程。

除此之外，在取证鉴定实践中还有几个位置我们不能忽略。例如 QQ 邮件信息，保存图片或截图的“Image”文件夹，默认存放接收文件的“FileRecv/My QQ file”文件夹等，同样可以获取到非常有价值的证据信息，且往往是聊天记录的重要补充或佐证。 如找到聊天记录中谈到的重要网银转账的操作界面截图，发现接收到的账单文件等。

对 QQ 邮件信息的取证鉴定与登陆口令相关，邮件内容存储在 QQ 服务器上，没有登陆口令想要获取邮件信息相对困难，但在取证实战中，我们可以结合

对浏览器缓存的取证，找到一些有用的邮件头信息或邮件内容信息。 如果一封邮件在本地打开过，就会在本机的浏览器缓存中留下一些邮件头或内容信息。 缓

存中的 QQ 邮件因为窗口格式问题可能会使得复原邮件信息位置重叠，难于查看，但对于取证鉴定来说，或许仅仅提取到一个邮件头信息就可能足以支撑起整个证据链。 因此，即使没有登录口令，我们在对 QQ取证的过程中也不能忽视邮件取证这个环节，最好在取证前就将其列入取证步骤计划。 对“Image”和“FileRecv/My QQ file”文件夹下文件信息的勘验和提取是取证鉴定实战中的常 用做法，因为每个 QQ 号码的“Image”文件下 保存着该号码接收到的一些图片、屏幕截图或 QQ 表情图片；而 “FileRecv”文件夹（QQ2008 版本为“My QQ file”文件夹）下保存着该号码默认接收到的各种类型文件，包括图片、文档、可执行文件、或是压缩文件包等，只要是按“发送文件”方式默认接收都将保存在此文件夹中。

## 联系运营商

### 公安调用QQ信息

往往在取证QQ聊天信息的时候，有关公安部门都有权调用QQ信息，这一方面可以获取信息，另一方面也可以对比云信息和本地信息是否一致，具有辅助验证的作用，因为不能排除嫌疑人伪造聊天记录的可能，需要第三方的验证。因此，运营商的帮助及其关键。

然后，查看有关问答律师的回复，他们对公安调取QQ聊天信息有如下解释：

1、可以调取，理由有多种，比如涉嫌刑事案件需要调取证据。

2、只要公安提出要求，运营商没有理由拒绝配合，运营商也没有权利和胆量要求公安说明详细原因，所以基本是无条件配合。

3、至于能调取多久的记录就要看运营商的技术能回力，真要认真去查，从你聊第一句的时答候开始都能查到。

### 法律依据

根据《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》

第三条 人民法院、人民检察院和公安机关有权依法向有关单位和个人收集、调取电子数据。有关单位和个人应当如实提供。

第一条 电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。电子数据包括但不限于下列信息、电子文件：

（一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；

（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；

（三）用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；

（四）文档、图片、音视频、数字证书、计算机程序等电子文件。

以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据，不属于电子数据。确有必要的，对相关证据的收集、提取、移送、审查，可以参照适用本规定

扩展资料

《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》

第十一条 具有下列情形之一的，经县级以上公安机关负责人或者检察长批准，可以对电子数据进行冻结：

（一）数据量大，无法或者不便提取的；

（二）提取时间长，可能造成电子数据被篡改或者灭失的；

（三）通过网络应用可以更为直观地展示电子数据的；

（四）其他需要冻结的情形。

第十二条 冻结电子数据，应当制作协助冻结通知书，注明冻结电子数据的网络应用账号等信息，送交电子数据持有人、网络服务提供者或者有关部门协助办理。解除冻结的，应当在三日内制作协助解除冻结通知书，送交电子数据持有人、网络服务提供者或者有关部门协助办理。

冻结电子数据，应当采取以下一种或者几种方法：

（一）计算电子数据的完整性校验值；

（二）锁定网络应用账号；

1. 其他防止增加、删除、修改电子数据的措施。

## 研究小结

QQ在过去的即时通讯当中是及其不安全，虽然现在有所改善，但依旧不是很完善。QQ和公安的关系也是十分的精密，有关网络诈骗的事件层出不穷，QQ需要公安来进行法律维护，同样，公安在处理有关刑事事件遇上信息获取困难的时候，也需要求助QQ提供技术帮助。所以在QQ取证方面，具有着得天独厚的特点。

本次研究对象，主要是从存储角度出发，有关文件、图像、聊天、联系人等信息存储位置以及获取方法来思考，并以实践为主，亲自的尝试QQ的各种功能来获取真实的数据。网上有着许多的过去QQ取证的方法，但是版本更新，以及信息的过于老旧，使得大部分都变得无用，这使得工作量变得很大。

同样也参考了知网上的两篇有关QQ取证的论文，但是有关这类的信息过于稀少，实在是令人叹息。