CTF隐写总结

原创

Sn0w/ 于 2019-04-06 14:30:44 发布 2400 收藏 39

文章标签： CTF隐写总结

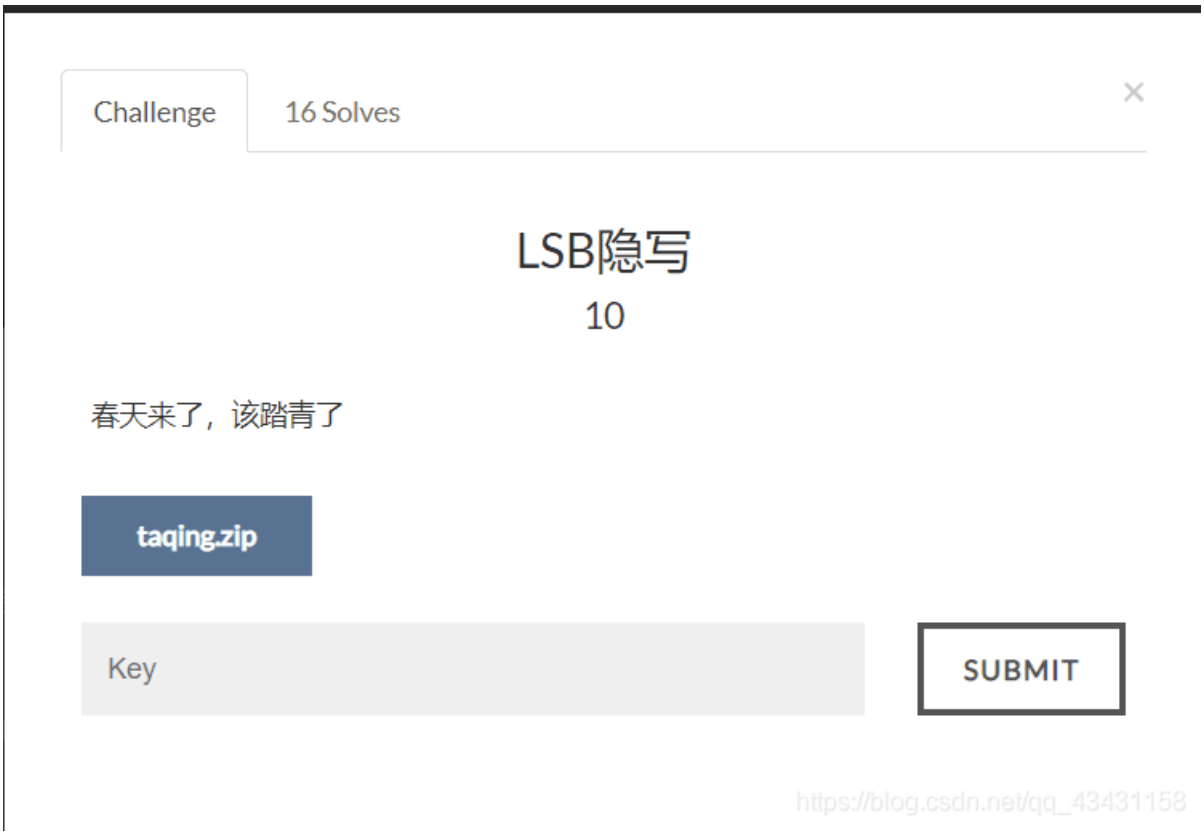
本文链接：https://blog.csdn.net/qq_43431158/article/details/89004457

CTF隐写总结

一：LSB隐写

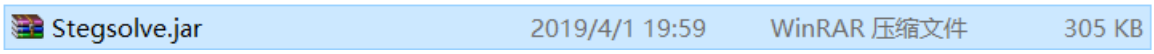
> **LSB概念**
> LSB，英文 least significant bit，中文义最低有效位。
> 对于一个给定的数据串,其最低有效位就是拥有最小单位数值的那一位.

关于LSB隐写的详细介绍 LSB详细介绍
关于LSB隐写的详细算法 LSB详细算法
关于LSB隐写的总结博客 LSB隐写总结
隐写技巧：PNG文件中的LSB隐写

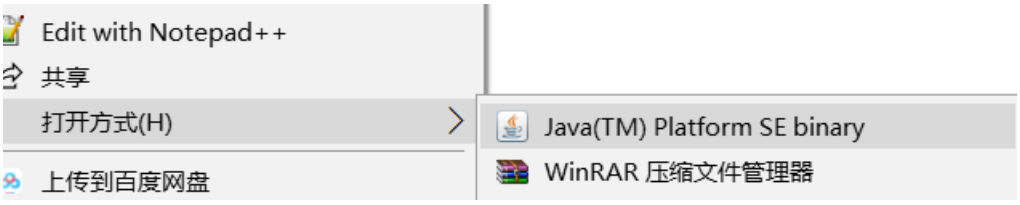


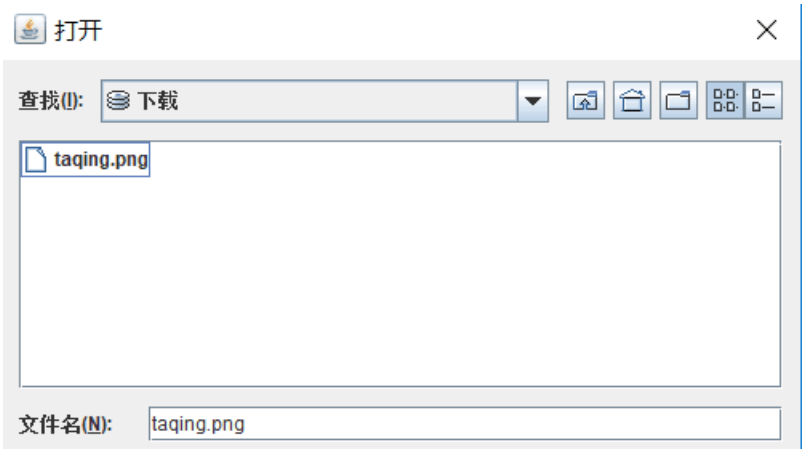
打开以后是一张这样的图片

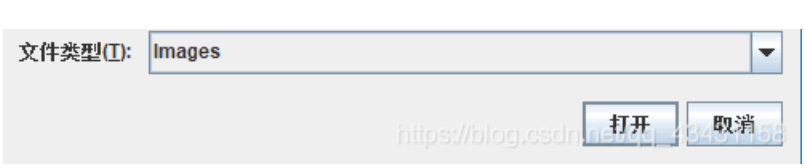
题目已经提醒这道题属于LSB隐写，那么就发动查百度、谷歌大法吧。
经过查找，会发现需要用这个神器来处理这种题目。



但打开这个软件需要有java，所以还得下载，最好也配置一下环境变量。
java详细配置
配置好之后那，用这种方式打开Stegsolve.jar

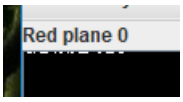




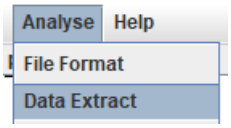


将图片打开后，通过下方的按钮切换不同的通道。结果你就会发现一个很不一样的东西。

红色通道前六张都没有太大的变化，但是问题出现在第七张。



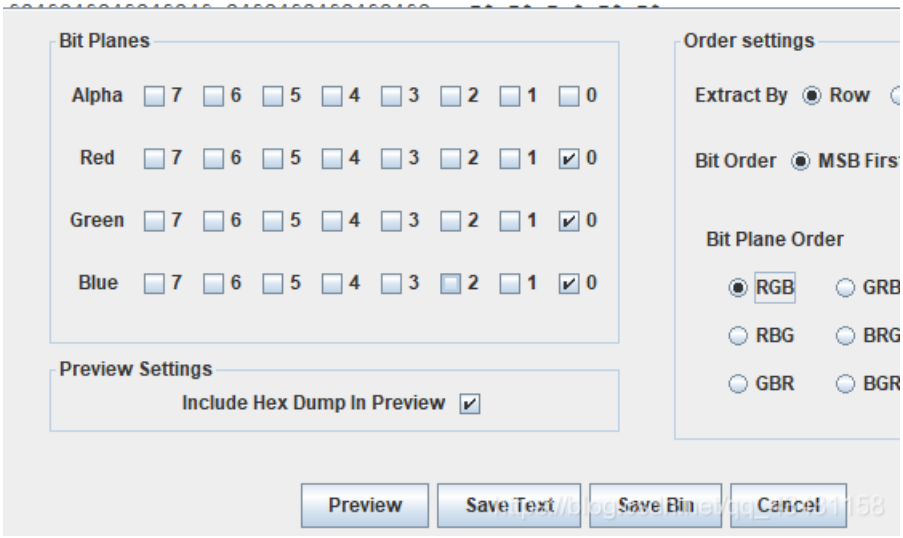
可以明显的看到，右上方隐藏了一些东西。
然后，通过观察，发现，green通道和blue通道也是如此。



那接下来就进行数据提取
因为发现三种颜色都是在0通道时发生了不同，所以勾选三个颜色的最低位。

```
666c61677b686176 65206120676f6f64  flag{hav e a good
2074696d65217d49 2492492492492492   time!}I $.I$.I$.
4924924924924924 9249249249249249  I$.I$.I$ .I$.I$.I
2492492492492492 4924924924924924  $.I$.I$. I$.I$.I$
9249249249249249 2492492492492492  .I$.I$.I $.I$.I$.
```

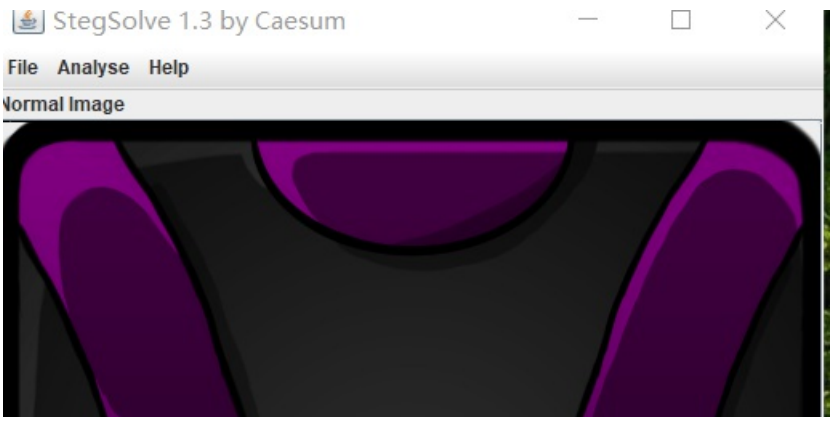
```
4924924924924924 9249249249249249  I$.I$.I$ .I$.I$.I
2492492492492492 4924924924924924  $.I$.I$. I$.I$.I$
9249249249249249 2492492492492492  .I$.I$.I $.I$.I$.
4924924924924924 9249249249249249  I$.I$.I$ .I$.I$.I
2492492492492492 4924924924924924  $.I$.I$. I$.I$.I$
```

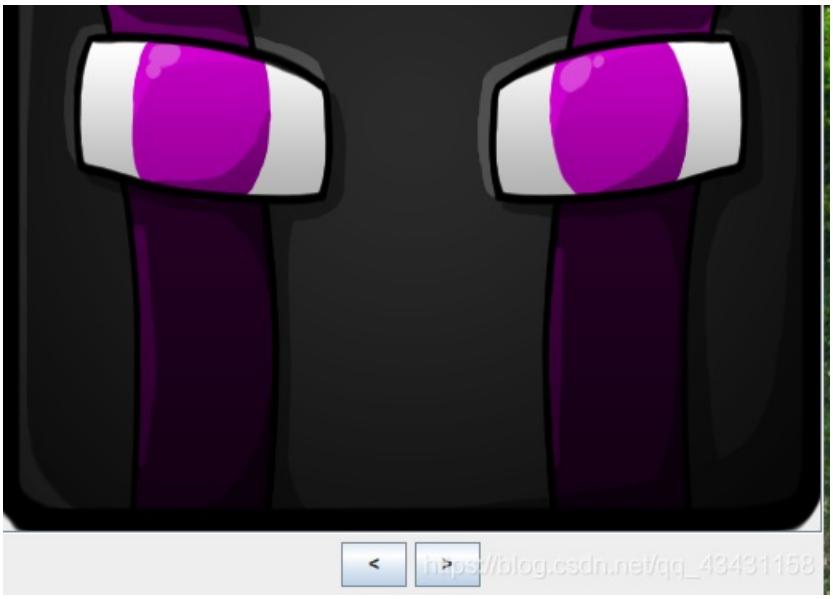


结果flag就出来咯！！

题是很简单，但关键是要理解为何如此做，做题不难，难在理解为何这样做。

大牛的博客——介绍为何勾选最低位的0

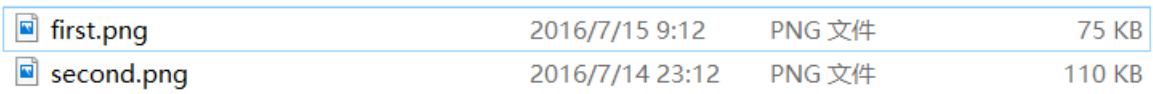


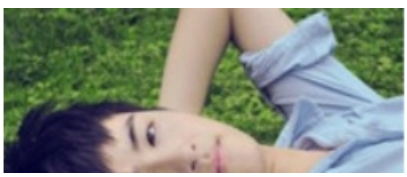


这道题的解法与上一道也是一样的。

二：双图

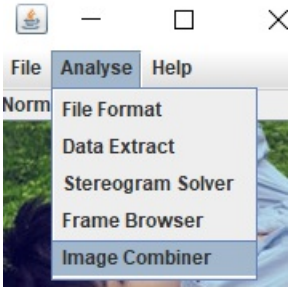
打开后是两张图片，而且两张图片一样。？？？这时就该敏感了，因为大多两张图片相同的题型都是**盲水印**，另外一种就是**双图**，但题目已经提示了是双图，所以就安装双图的做法去解决这道题。



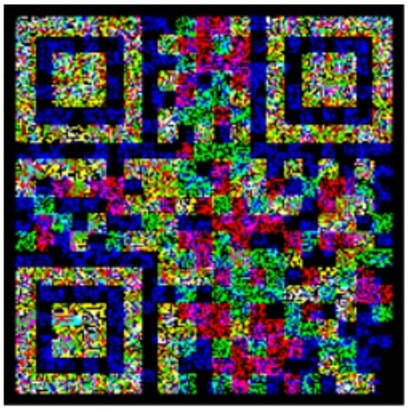


（两张图片大小不一样，第二张一定隐藏了一些信息）
用Stegsolve打开第一张图

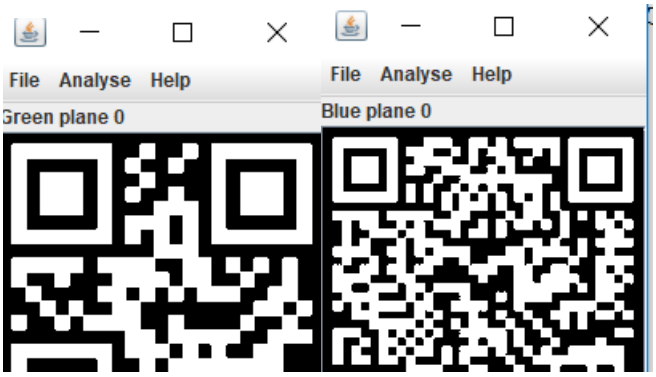
再使用Image combiner(图像结合),与第二张结合，看看会发生什么变化。（**我觉得这里就是两张图片进行对比，前面可以看到第二张图片比第一张图片大了30多KB，所以那多出的30多KB的内容会出现在结合后的图片中**）

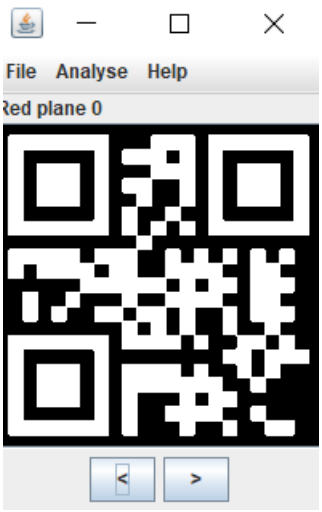


结果在变换通道中找到一个二维码，扫吧。。。结果什么也扫不出了。。。



将这张图片保存下来，再用Stegsolve打开，变换通道，可以看到三张不同的二维码。





下面就是扫码工作了，(推荐支付宝扫码，微信我半天都没扫出来，还以为错了。。。)扫过之后，有提示，有密文，解密就能得出flag了

三：盲水印

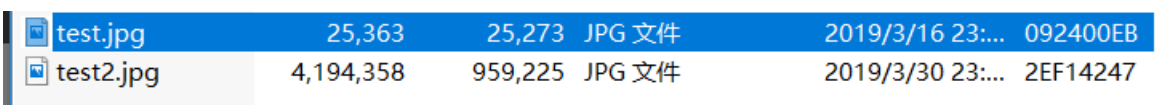
> **盲水印介绍：**
> 盲水印隐蔽性强，给水印数据进行编码过后不易被破解出来，而且不会破坏图片美观，且又能很好的保护图片版权。

详细介绍盲水印的一些博客：

介绍盲水印

盲水印原理

打开之后是两张相同的图片



发动查百度、谷歌大法，破解盲水印，需要脚本或工具。

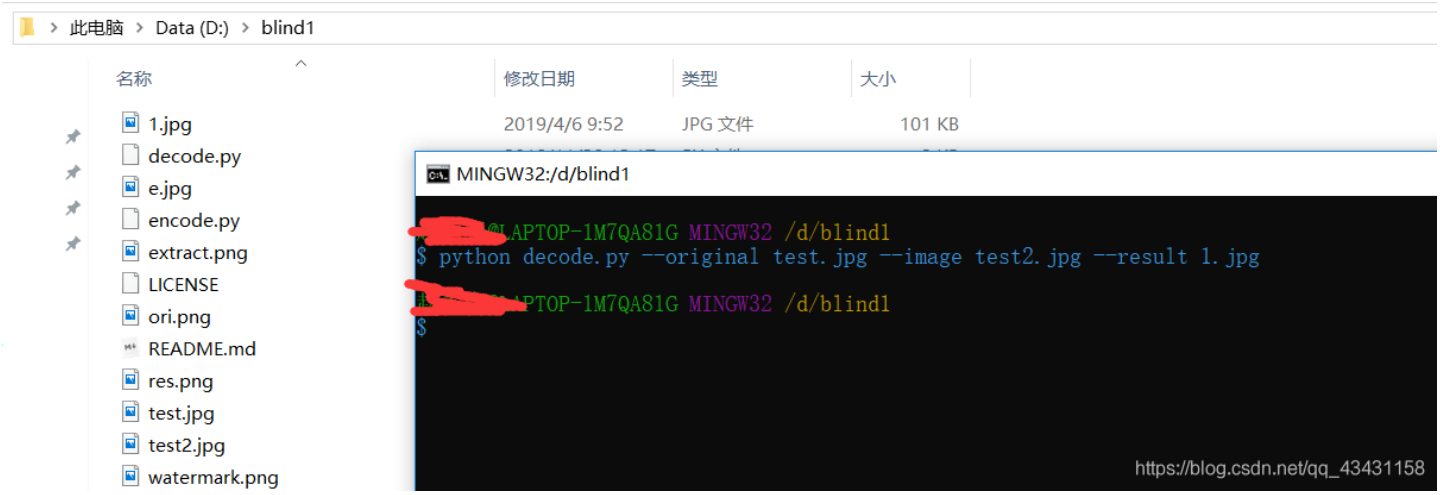
BlindWaterMark脚本
但要注意这个是py2的脚本，如果下载的是py3就会出现语法错误。（这里卡了我一晚上）

修改方法是：py3自带了一个脚本2to3.py，可以将python2的程序自动转为python3的形式。但是不熟悉python语法，到后面还是会出现错误。（**所以最好先不要用这个脚本去解题，待熟悉python语言后再用，否则就算知道哪里错了，也不会改**）大牛的博客介绍如何修改

这里介绍另一个脚本
blind-watermark
这个脚本可以选择下载py3的脚本，这样就可以减少一些修改麻烦。

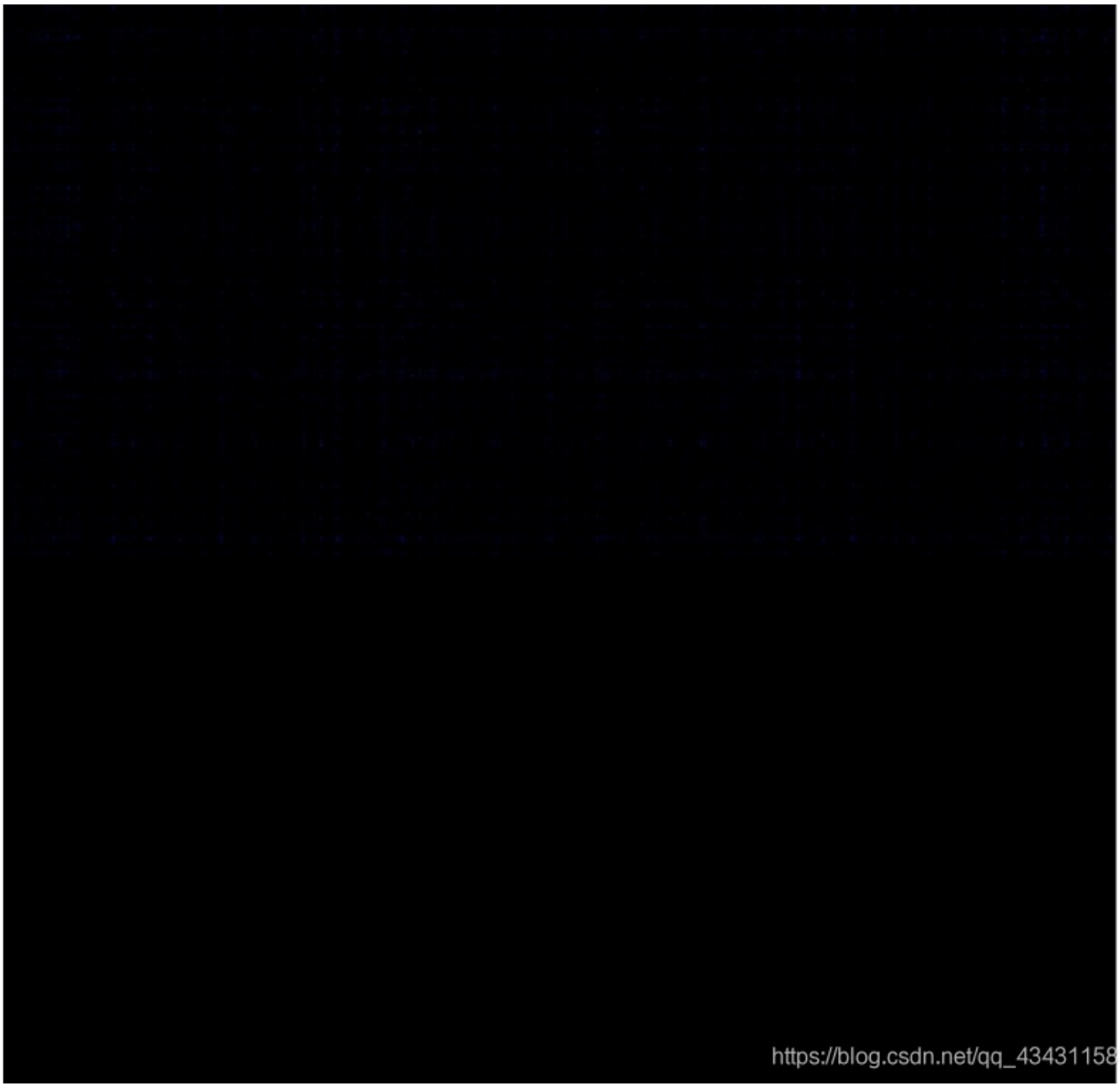
> 操作语法
> python decode.py --original ori.png --image res.png --result extract.png
> 注意： 两张图片分辨率要相同，否则会报错。

在下载脚本的目录里打开cmd，输入命令。



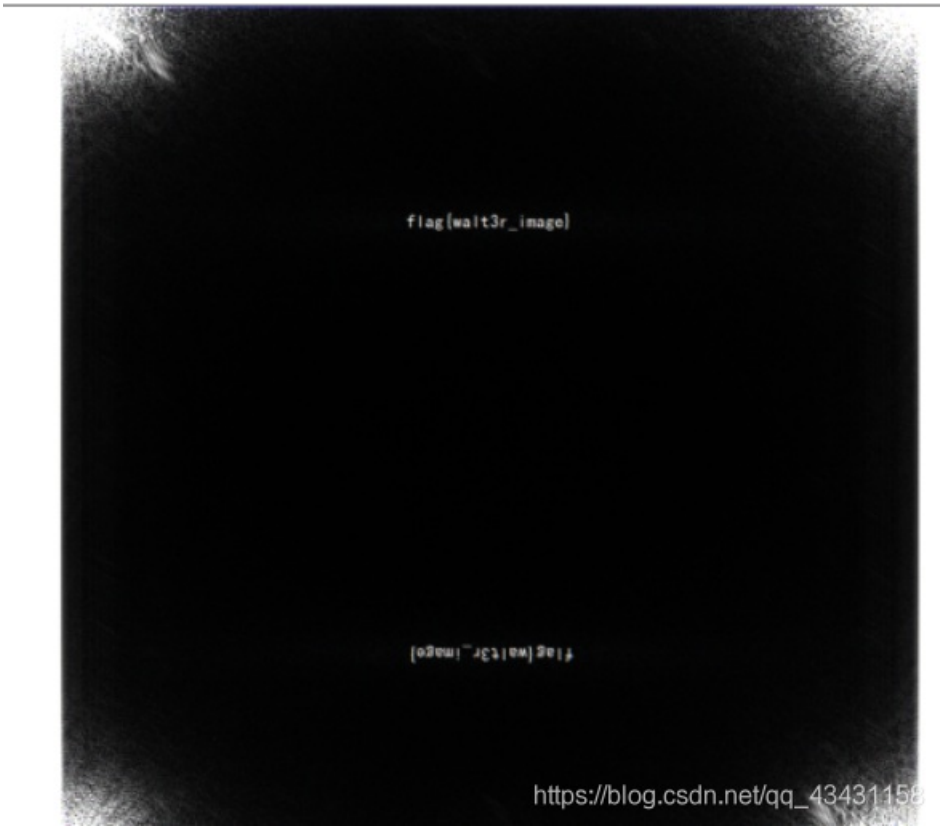
出现一个图片，但是打开却。。。

黑黑的。。。啥也看不见。。。



既然脚本这条路走不通，那只好偷懒了，下载工具吧。
数字盲水印&隐形水印制作工具WaterMarkH V1.2下载地址

两张图片相同，一定是图片大的那一张隐藏有信息，所以试试第二张。



flag出来了(**感悟：有时如果是脚本对图片进行盲水印的话，那只能用脚本才能解开。但如果用工具添加水印的话，也只能用工具解开**)

四：画图

Drawing

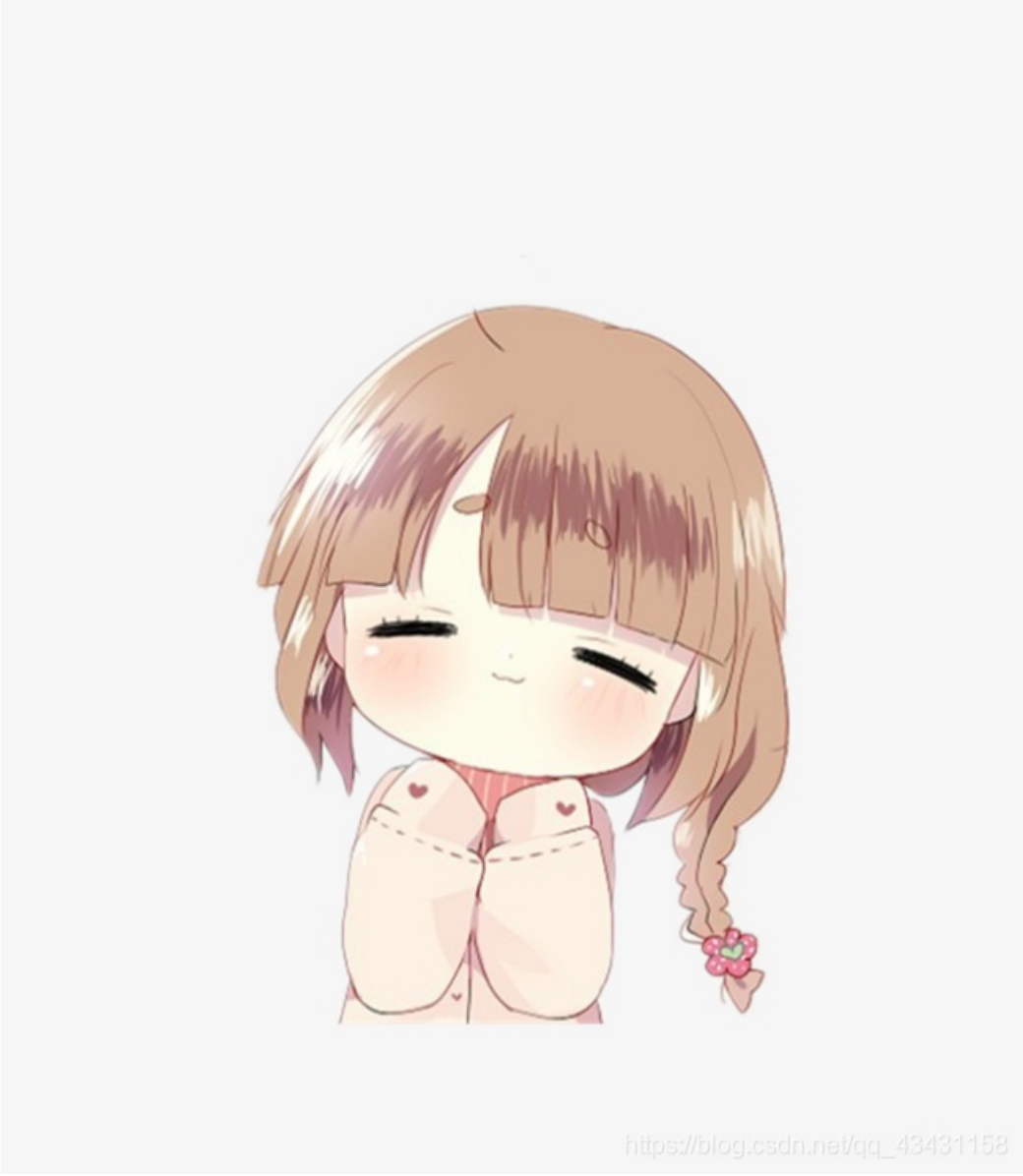
zip

Key

SUBMIT

paint.png 2019/4/2 20:22 PNG 文件 818 KB

打开以后是一个很可爱的女孩子



用Winhex打开图片，发现有很大的不同，上面全是乱码，但是到了下面全是数字，估计藏有猫腻。

```
lA    € $  œ ¨Ü9å–¶J
l8 @    € TnË€ $    H
)1  ' *wN¹¥–  € $
```

```
•Û2    H@   È‰€Ê S
ni« $    H@å¶ H@
  € r" rç”[Ú*  H
@  P¹-    € $  œ
¨Ü9å-¶J@    € TnË
€ $    H ' *wN¹¥-
  € $  •Û2    H@
 È‰€Ê Sni« $    H
@å¶ H@    € r" rç
”[Ú*  H@  P¹-
€ $  œ ¨Ü9å-¶J@
  € TnË€ $    H '
 *wN¹¥-  € $  •Û
2    H@  È‰€Ê Sni
« $    H@å¶ H@
€ r" rç”[Ú*  H@
 P¹-    € $  œ ¨Ü
9å-¶J@    € TnË€
$    H ' *wN¹¥-
€ $  •Û2    H@  È
‰€Ê Sni« $    H@å
¶ H@    € r" rç”[
Ú*  H@  P¹-    €
$  œ ¨Ü9å-¶J@
€ TnË€ $    H ' *
wN¹¥-  € $  •Û2
  H@  È‰€Ê Sni«
$    Hày  §¦àkI
     IEND®B`‚2837
2c37290a28372c38
290a28372c39290a
28372c3130290a28
372c3131290a2837
2c3132290a28372c
3133290a28372c31
34290a28372c3135
290a28372c313629
0a28372c3137290a
28372c3138290a28
372c3139290a2837
2c3230290a28372c
3231290a28372c32
32290a28372c3233
```

ctrl+A全选，然后再将这一堆数字给复制出来

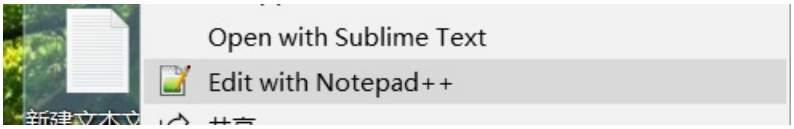
新建文本文档 (2).txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

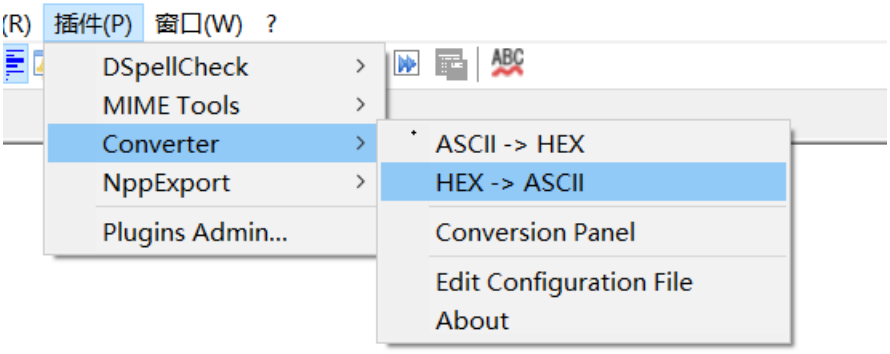
```
3290a283236302c313634290a283236302c313635290a283236302c313636290a28323
)a283236302c323636290a283236302c323637290a283236302c323638290a283236302
12c313632290a283236312c313633290a283236312c313634290a283236312c3136352
23634290a283236312c323635290a283236312c323636290a283236312c323637290a2
)a283236322c313631290a283236322c313632290a283236322c313633290a283236322
236322c323633290a283236322c323634290a283236322c323635290a283236322c323
13539290a283236332c313630290a283236332c313631290a283236332c313632290a2
1290a283236332c323632290a283236332c323633290a283236332c323634290a28323
236342c313538290a283236342c313539290a283236342c313630290a283236342c313
42c323630290a283236342c323631290a283236342c323632290a283236342c3236332
6352c3531290a283236352c3532290a283236352c3533290a283236352c3534290a2832
.83236352c323132290a283236352c323133290a283236352c323134290a283236352c3
c3336290a283236362c3337290a283236362c3338290a283236362c3339290a2832363
```

```
3290a283236362c313834290a283236362c313835290a283236362c323031290a28323
1290a283236372c3232290a283236372c3233290a283236372c3234290a283236372c32
c313535290a283236372c313536290a283236372c313732290a283236372c313733290
731290a283236382c37290a283236382c38290a283236382c39290a283236382c31302
236382c313238290a283236382c313433290a283236382c313434290a283236382c313
82c323434290a283236382c323435290a283236382c323436290a283236382c3234372
83236392c3439290a283236392c3530290a283236392c3531290a283236392c3532290a
83236392c323130290a283236392c323131290a283236392c323132290a283236392c3
7302c3334290a283237302c3335290a283237302c3336290a283237302c3337290a2832
1290a283237302c313832290a283237302c313833290a283237302c313834290a28323
c3139290a283237312c3230290a283237312c3231290a283237312c3232290a2832373
c313533290a283237312c313534290a283237312c313535290a283237312c313536290
639290a283237312c323730290a283237312c323731290a
```


再用Notepad++打开



提示的是画图，在坐标系里画图需要坐标，现在给的一堆数字是十六进制的数，在Notepad++中转换一下，看是否能出现坐标。



结果确实出现了坐标

```
(271,128)
(271,143)
(271,144)
(271,145)
(271,146)
(271,147)
(271,148)
(271,149)
(271,150)
(271,151)
(271,152)
(271,153)
(271,154)
(271,155)
(271,156)
```

```
(271,172)
(271,173)
(271,174)
(271,175)
(271,176)
(271,177)
(271,178)
(271,179)
(271,180)
(271,181)
```

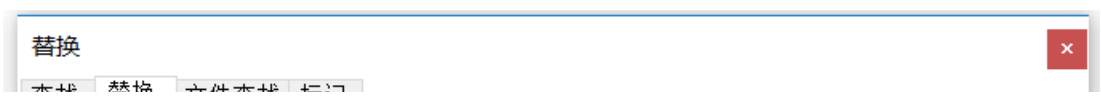
那下面就实现画图吧，怎么画。。。我还是去找百度、谷歌吧

经过查找需要这个画图工具

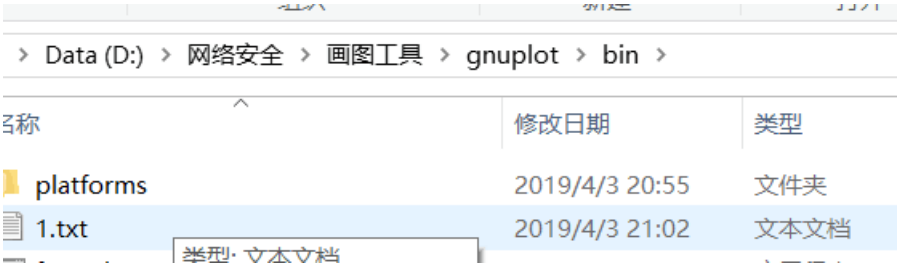
但是得注意一点的是，坐标必须满足这个工具的格式。必须改为这种格式的坐标

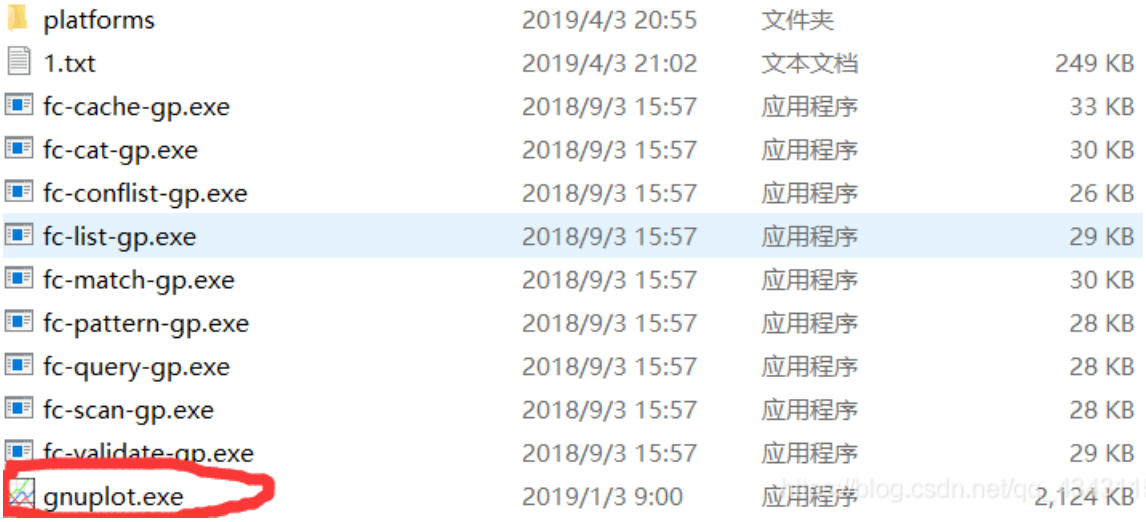
```
7 7
7 8
7 9
7 10
7 11
7 12
7 13
7 14
7 15
7 16
7 17
7 18
7 19
7 20
7 21
7 22
7 23
7 24
7 25
7 26
7 27
7 28
7 29
7 30
7 31
7 32
7 33
7 34
7 35
7 36
7 37
7 38
7 39
7 40
7 41
```

改成这样很简单，只需要点击替换，把（ 和）都替换掉，把逗号改为空格就了。



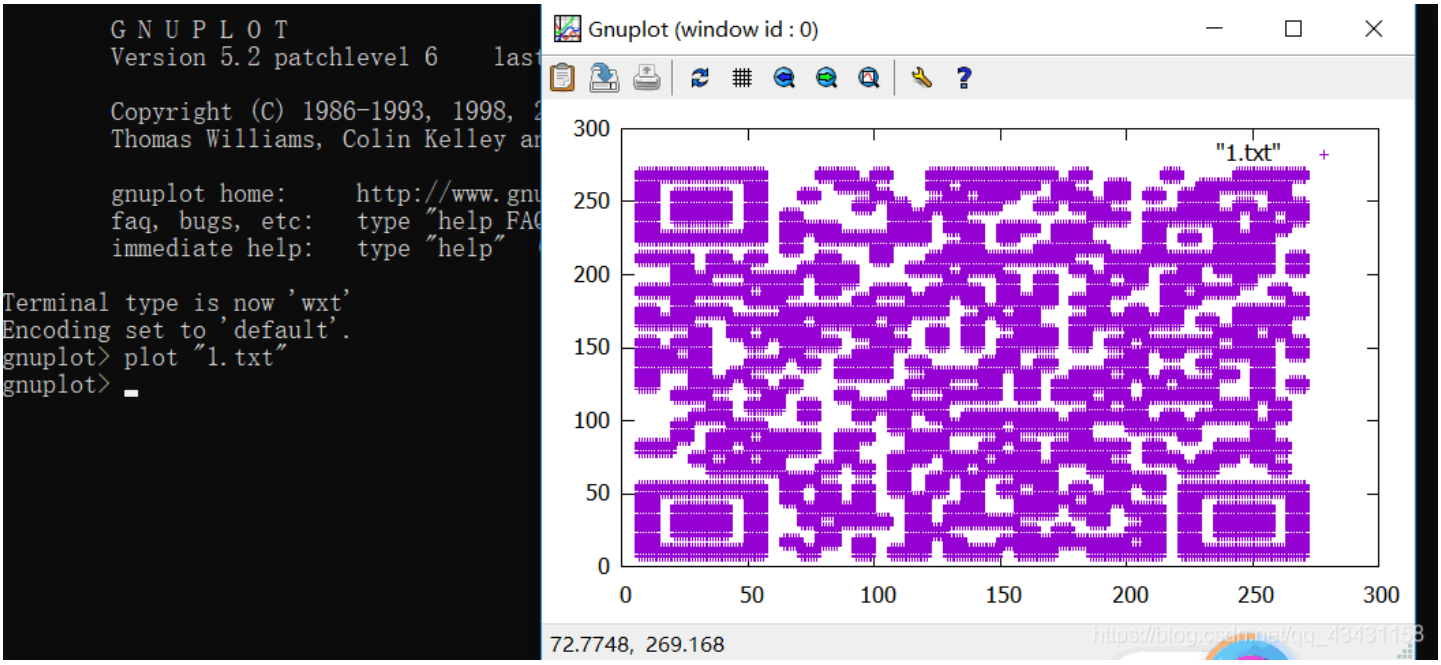
然后将改好的文档保存，放入gnuplot的bin目录里，打开bin目录gnuplot.exe，输入命令（我理解的是要执行的文件必须和这应用程序放在同一个目录，否则无法执行，会报错).





输入命令

```
plot “文件名”
```


G N U P L O T
Version 5.2 patchlevel 6
Copyright (C) 1986-1993, 1998,
Thomas Williams, Colin Kelley a
gnuplot home:
faq, bugs, etc:
immediate help:
Terminal type is now 'wxt'
Encoding set to 'default'.
gnuplot> plot "1.txt"
gnuplot>
Gnuplot (window id : 0)
"1.txt"
300
250
200
150
100
50
0
0
50
100
150
200
250
300
72.7748, 269.168

用支付宝一扫就?了


https://blog.csdn.net/qq_43431158