西邮网络科技协会ctf平台misc之真假迪迦writeup

原创

百里小羊 于 2019-11-16 14:10:27 发布 482 收藏 2

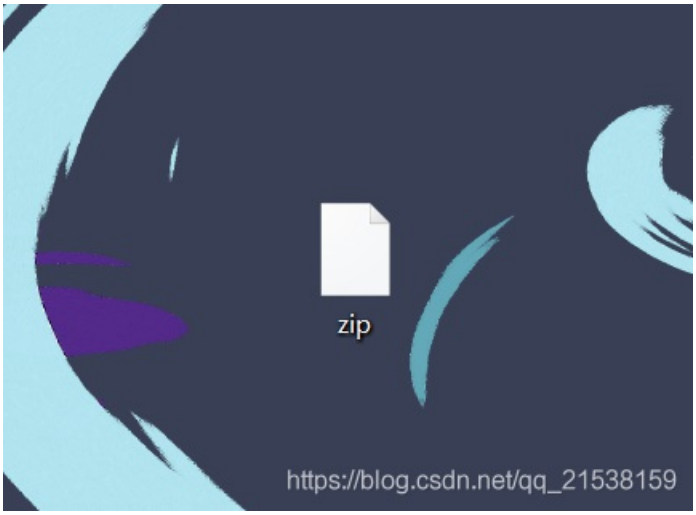
先来看题！！！

这里划重点

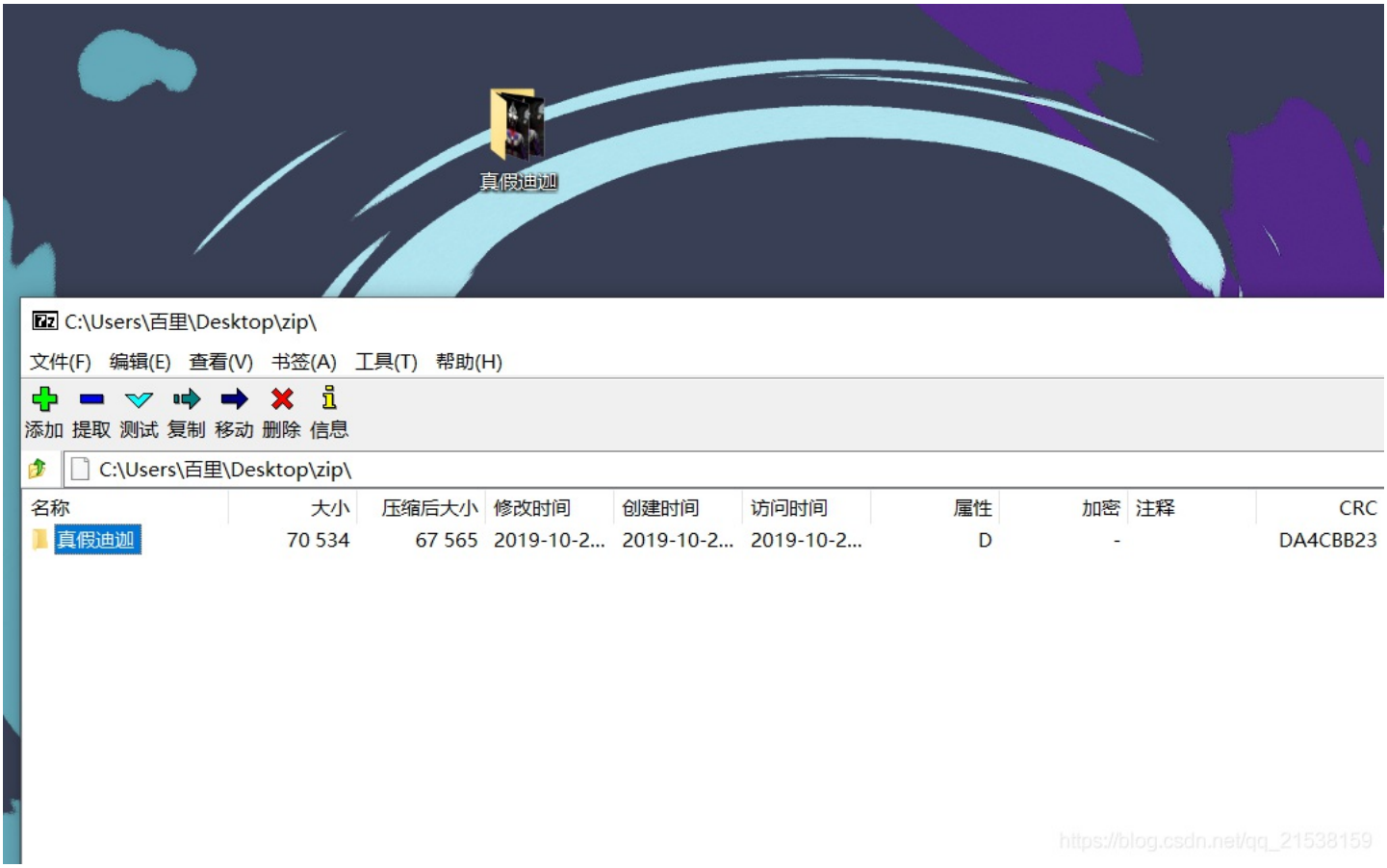
ll学长会为找到的人送出惊喜哦！

冲

下载压缩包



直接7z，拖拽解压



打开以后是两张图片

依次看下文件大小，再放winhex下看下，尝试搜索flag关键字字段未果，于是乎直接binwalk一下(这里为了方便直接改成1.jpg，和2.jpg)

```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
32322         0x7E42          Zip archive data, at least v2.0 to extract, compressed size: 896, unc
ompressed size: 65536, name: flag1.txt
33348         0x8244          End of Zip archive, footer length: 22

root@kali:~#
```

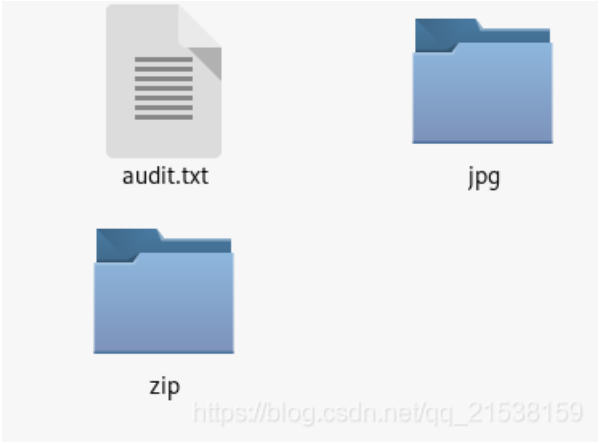


```
root@kali:~# binwalk '/root/2.jpg'

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01

root@kali:~#
```

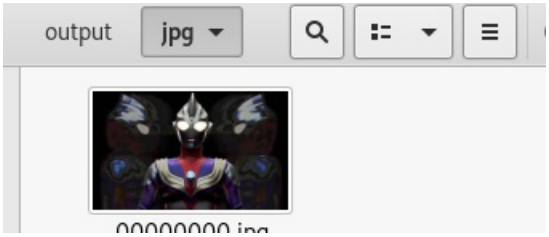
果然第一张图有东西，然后借助**foremost**工具分离一下

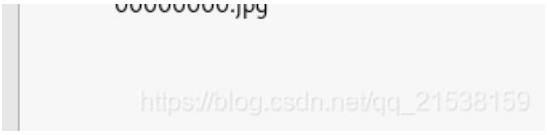
```
root@kali:~# foremost '/root/1.jpg'
Processing: /root/1.jpg
|foundat=flag1.txt
```


这里看到flag1.txt字段
同时在当前文件夹下生成一个output文件夹，内容如下

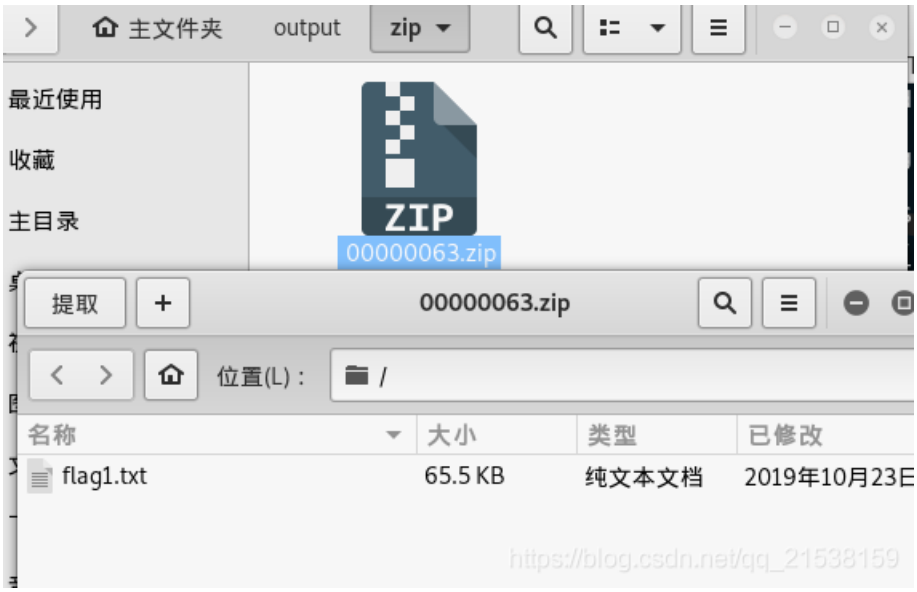


jpg里因该是迪迦的原图了

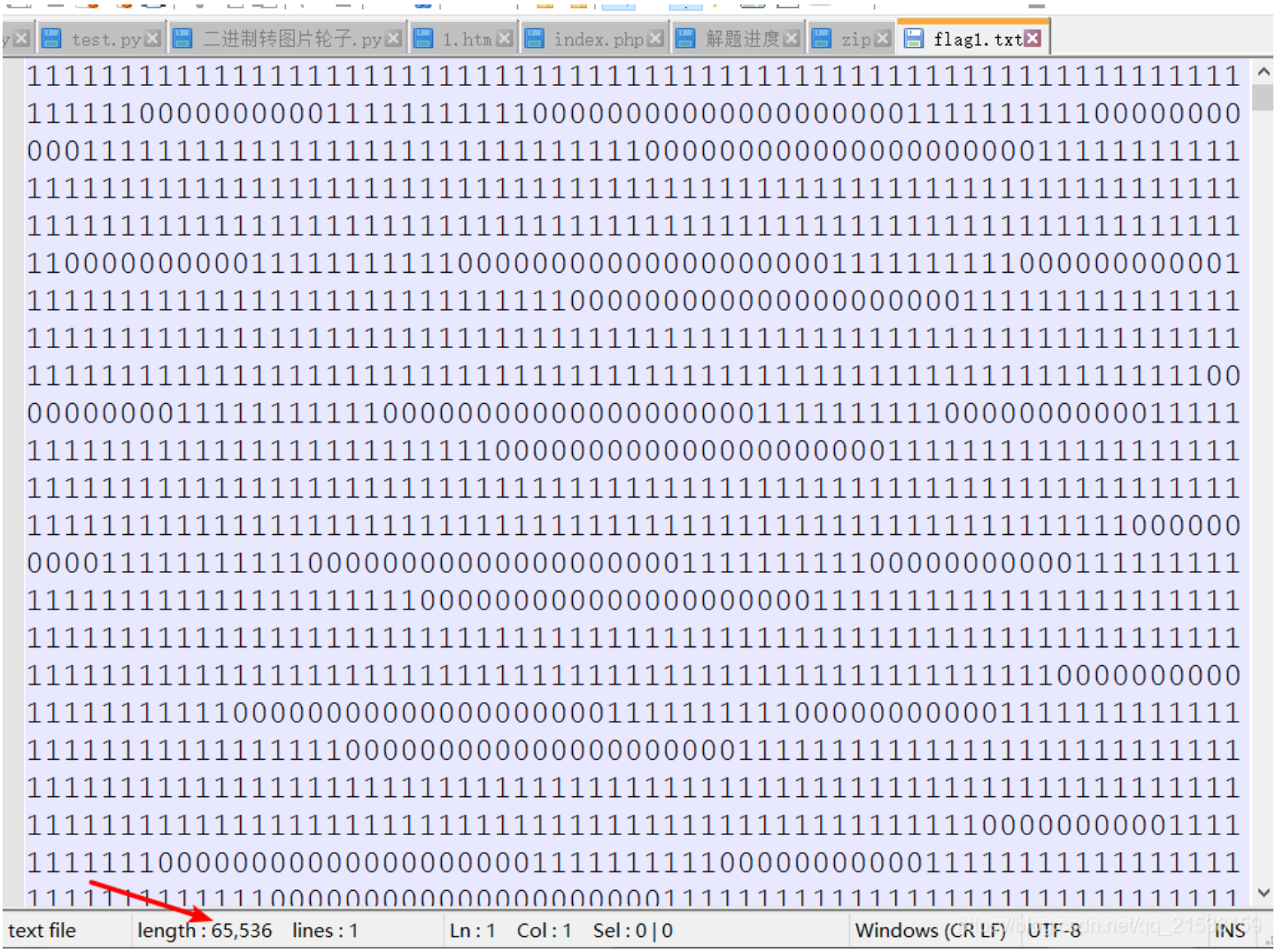




zip解压后发现flag1.txt



跟进flag1.txt



这里注意两点

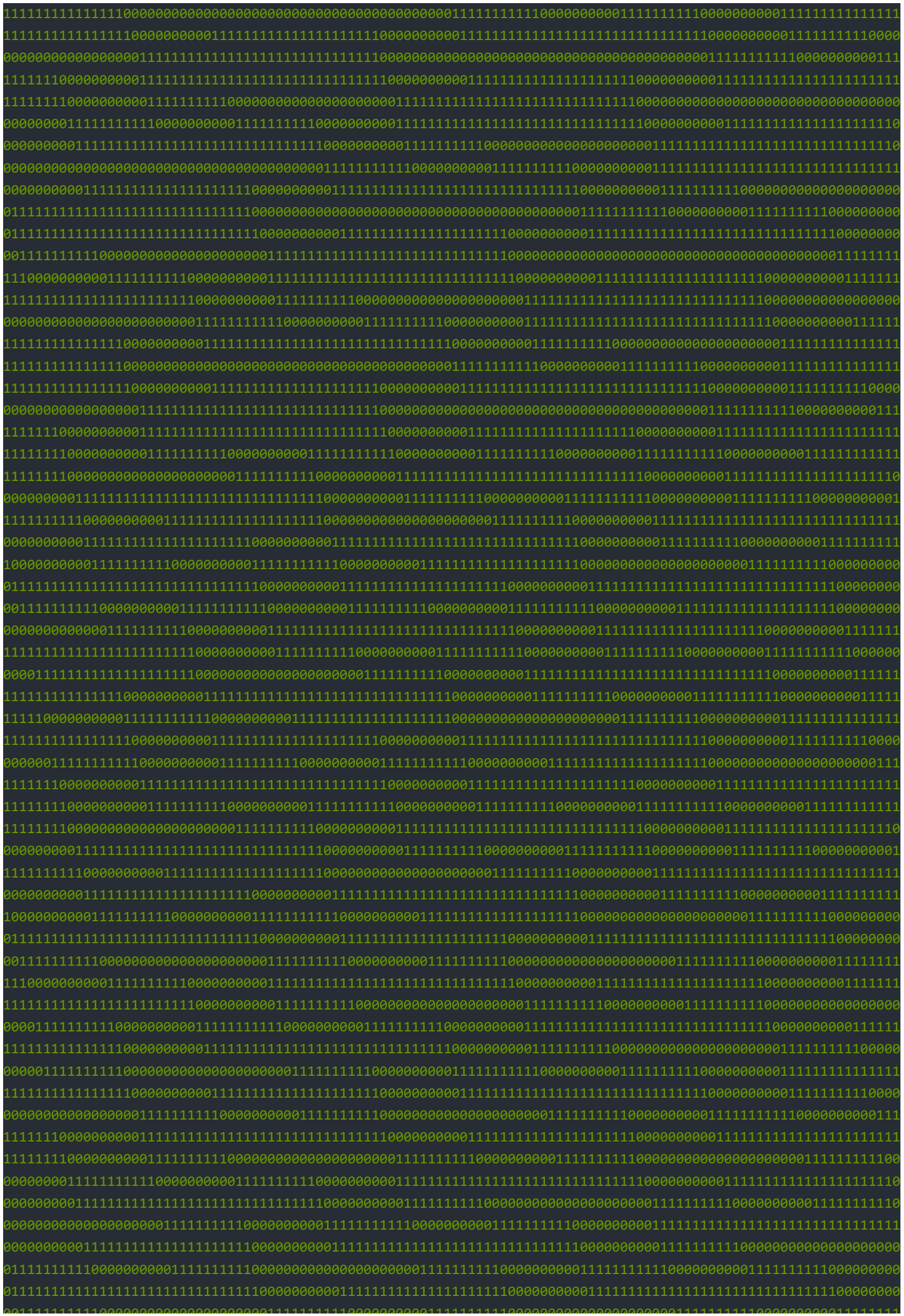
其一 全部为二进制0，1数据

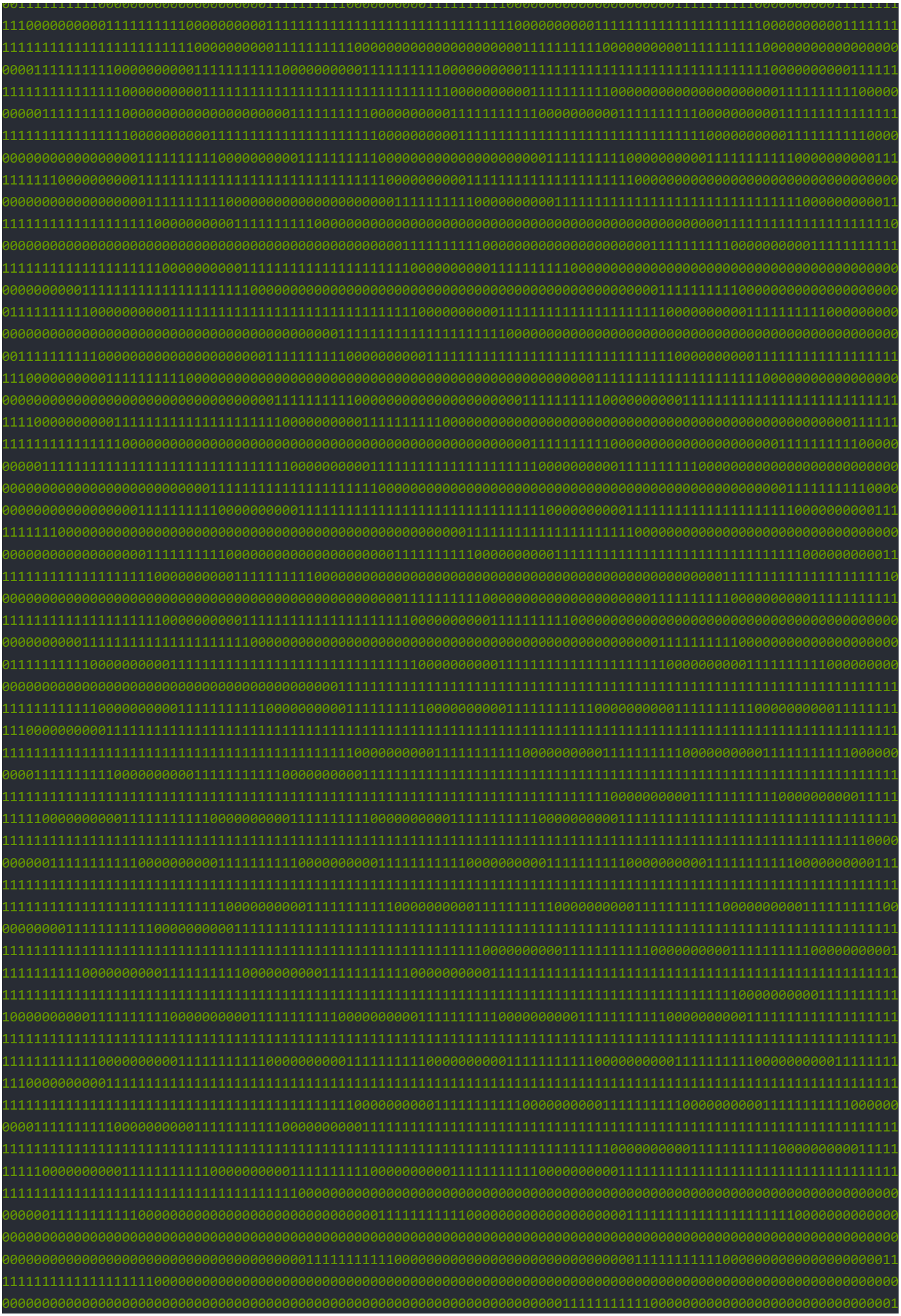
其二 总二进制比特流共65536位，也就是256 X 256

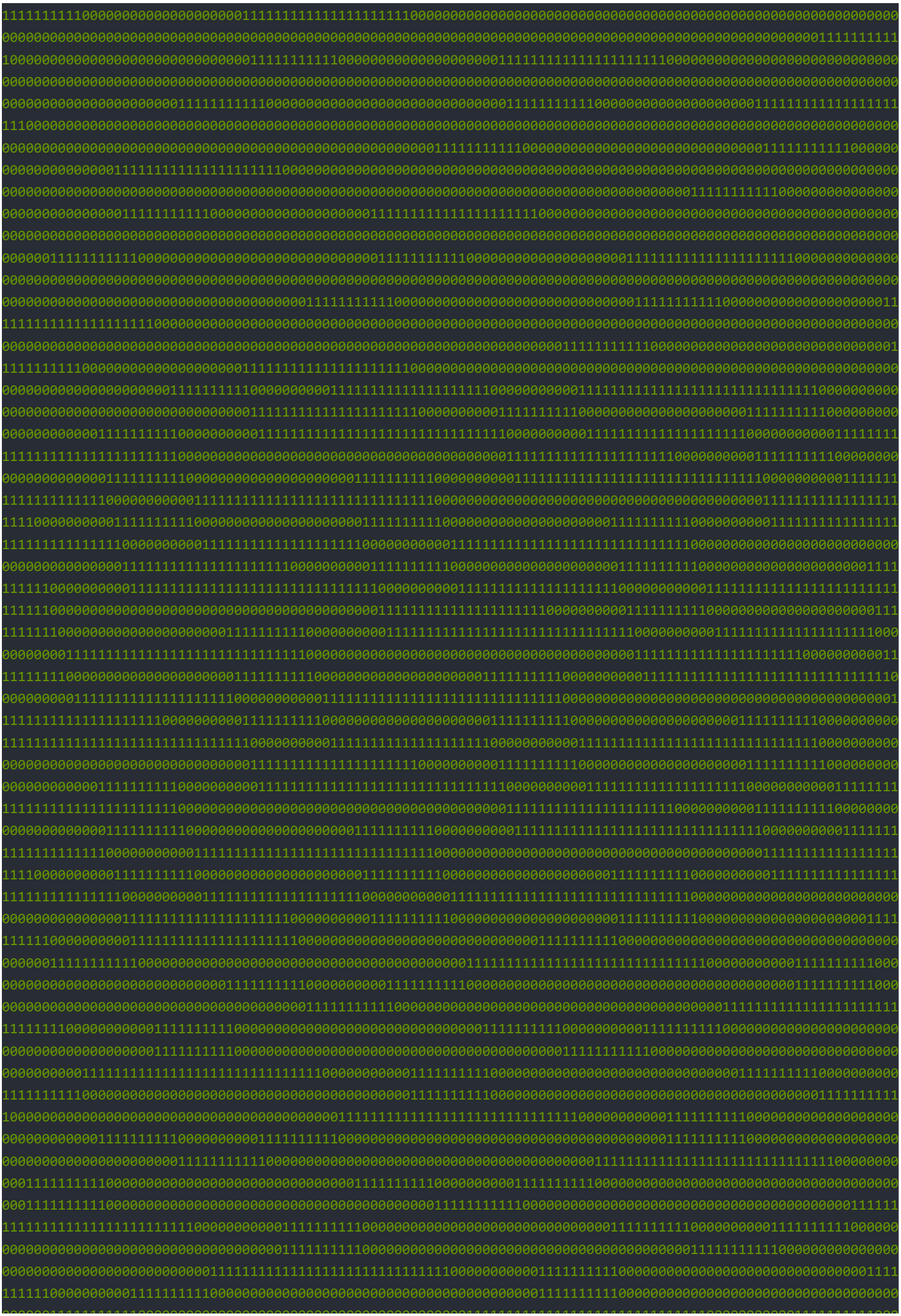
那就差不多是要把它转化成二维码了

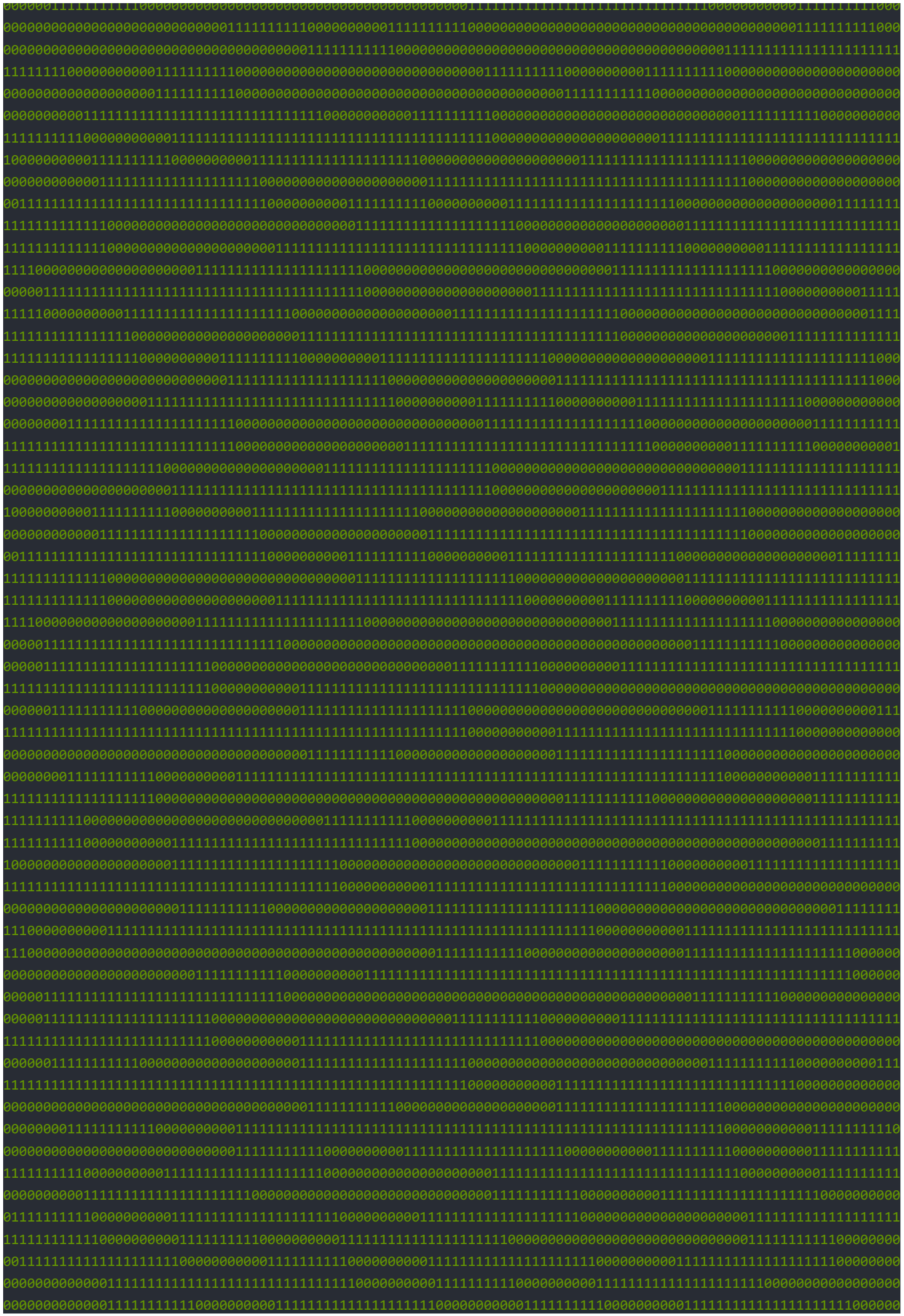
代码如下

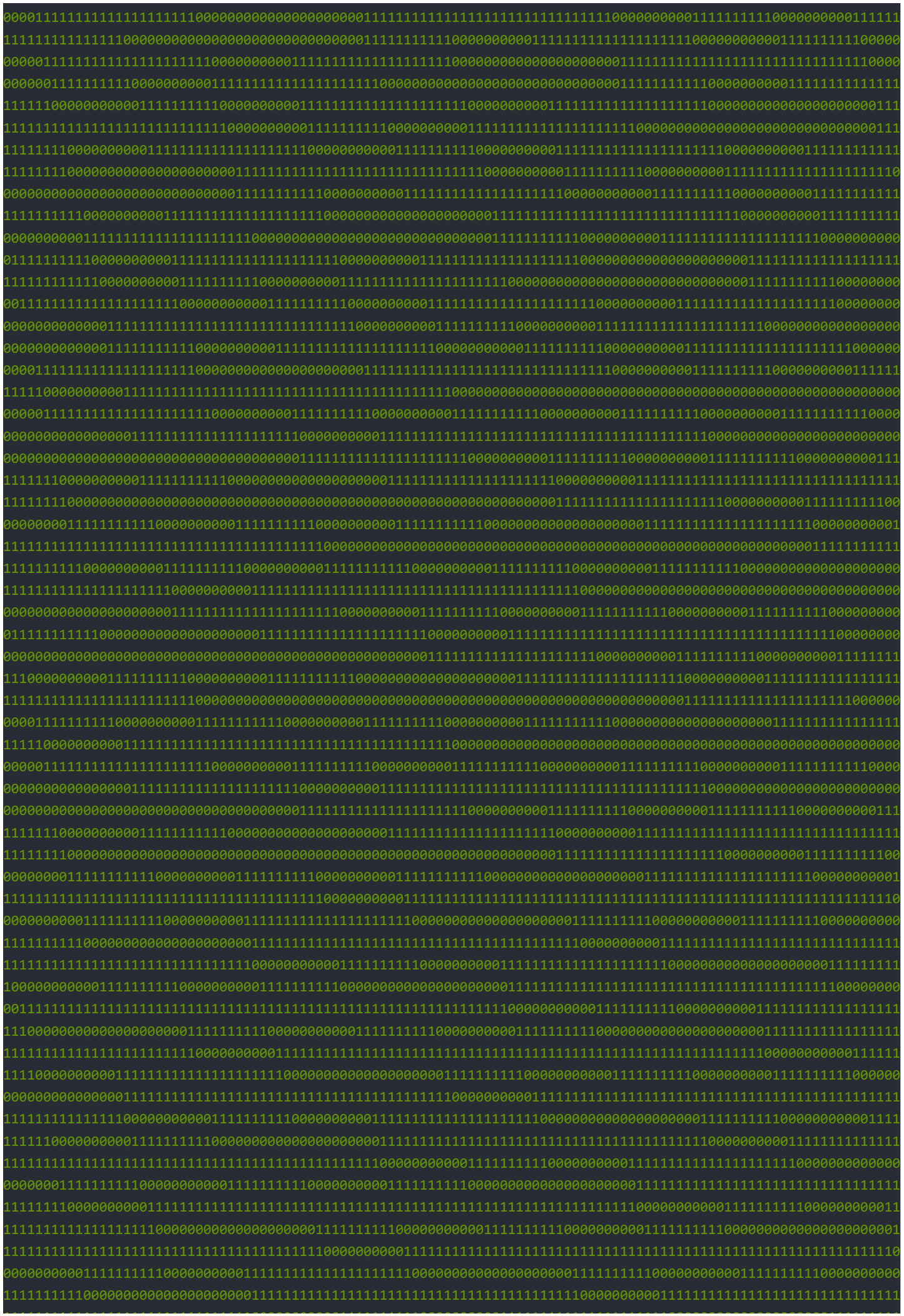
```
import PIL
from PIL import Image
MAX = 256
img = Image.new("RGB",(MAX,MAX))
str="111111111111111111111111111111111111111111111111111111111111111111111111111000000000111111111100000000000000000
00000111111111100000000001111111111111111111111111111110000000000000000000000111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111110000
00000011111111110000000000000000000111111111100000000000111111111111111111111111111110000000000000000000000000111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111100000000001111111111000000000000000000000111111111100000000000111111111111111111111111
11111111000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111100000000001111111111000000000000000000001111111111110
00000000011111111111111111111111111111100000000000000000000001111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111000000000111111111
10000000000000000000011111111110000000000011111111111111111111111111111000000000000000000000111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111110000000000111111111100000000000000000000111111111100000000000111111111111111111111111111111100000000
00000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111000000000011111111110000000000000000000011111111110000000000111111
11111111111111111111111110000000000000000000001111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111100000000001111111111000000000000000
00000111111111100000000001111111111111111111111111111110000000000000000000000111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111110000
00000011111111110000000000000000000111111111100000000000111111111111111111111111111110000000000000000000000000111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111100000000001111111111000000000000000000000111111111100000000000111111111111111111111111
11111111000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111110
00000000000000000000000000000000000000000000000000111111111100000000001111111111000000000000000000001111111111
11111111111111111111100000000000000000000111111111100000000001111111111000000000000000000000000000000000000000000
00000000011111111111111111111000000000000000000000000000000000000000000000000000111111111000000000011111111111
10000000000000000000011111111111111111111111111111100000000000000000000001111111111100000000001111111111000000000
00000000000000000000000000000000000000000000111111111111111111111000000000000000000000000000000000000000000000000
00111111111100000000001111111111000000000000000000000111111111111111111111111111111100000000000000000000011111111
11100000000000111111111100000000000000000000000000000000000000000000000000111111111111111111111100000000000000000
00000000000000000000000000000000000000111111111100000000001111111111000000000000000000001111111111111111111111111111
11110000000000000000000011111111110000000000111111111100000000000000000000000000000000000000000000000000000011111111
11111111111111100000000000000000000000000000000000000000000000000000001111111111000000000011111111110000000000000000
00000111111111111111111111111111111100000000000000000000001111111111100000000000111111111100000000000000000000000000
00000000000000000000000000011111111111111111111110000000000000000000000000000000000000000000000000000111111111100000
00000011111111111000000000000000000000011111111111111111111111111111110000000000000000000000111111111100000000000111
11111100000000000000000000000000000000000000000000000000000000111111111111111111111110000000000000000000000000000000
00000000000000000011111111110000000000111111111110000000000000000000011111111111111111111111111111111110000000000000
00000000111111111110000000000111111111100000000000000000000000000000000000000000000000000111111111111111111111110
00000000000000000000000000000000000000000000000000111111111100000000001111111111000000000000000000000011111111111
11111111111111111111000000000000000000000111111111100000000001111111111000000000000000000000000000000000000000000
00000000011111111111111111111000000000000000000000000000000000000000000000000000111111111000000000011111111111
10000000000000000000011111111111111111111111111111100000000000000000000001111111111100000000001111111111000000000
00000000000000000000000000000000000000000000111111111111111111111000000000000000000000000000000000000000000000000
00111111111100000000001111111111000000000000000000000111111111111111111111111111111100000000000000000000011111111
11100000000000111111111100000000000000000000000000000000000000000000000000111111111111111111111100000000000111111
1111111111111111111111110000000000111111111100000000000000000000001111111111111111111111111111111111000000000000000000
000000000000000000000000011111111110000000000111111111100000000000111111111111111111111111111111111100000000000111111
111111111111111000000000011111111111111111111111111111111110000000000111111111100000000000000000000001111111111111111
```

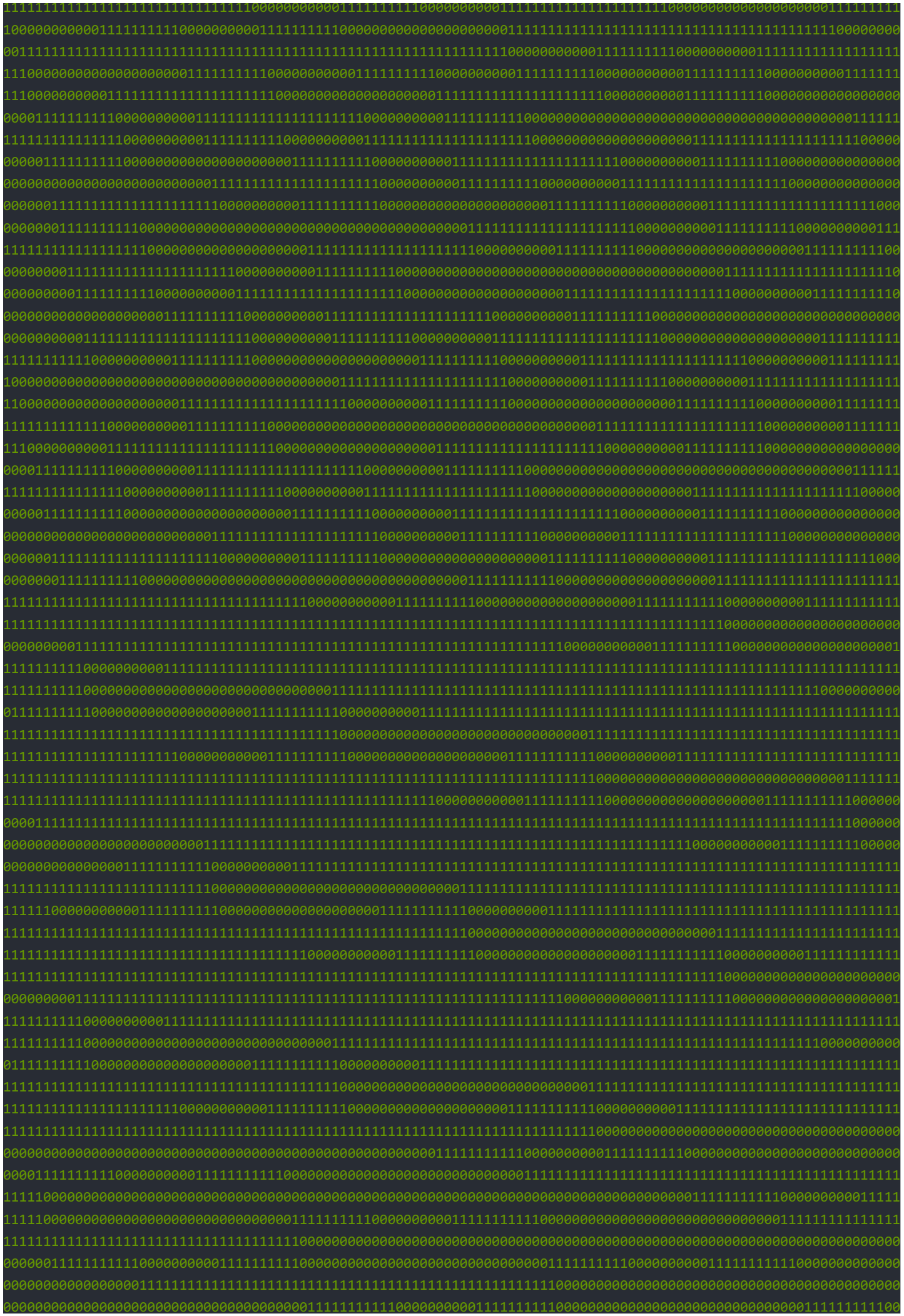


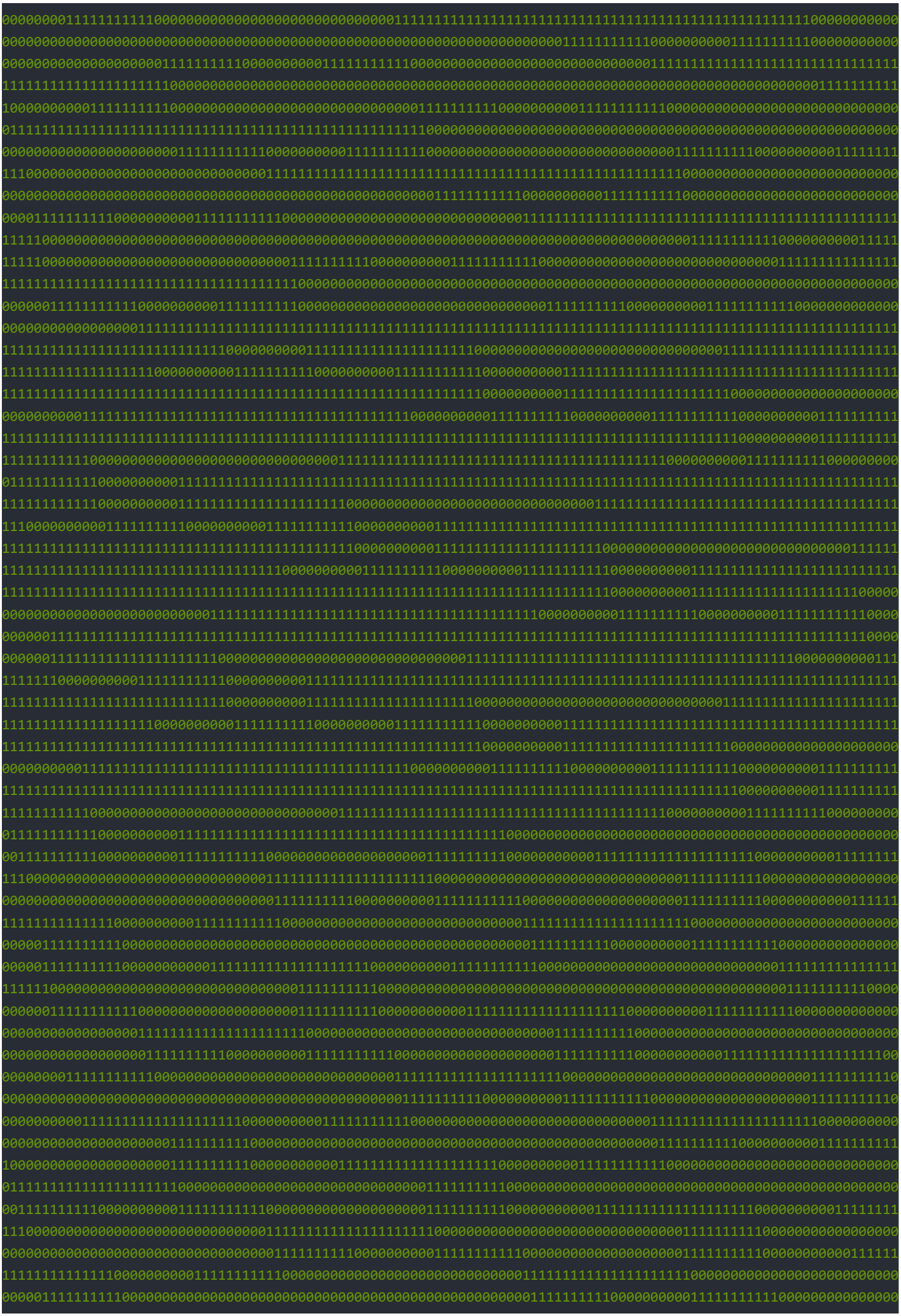


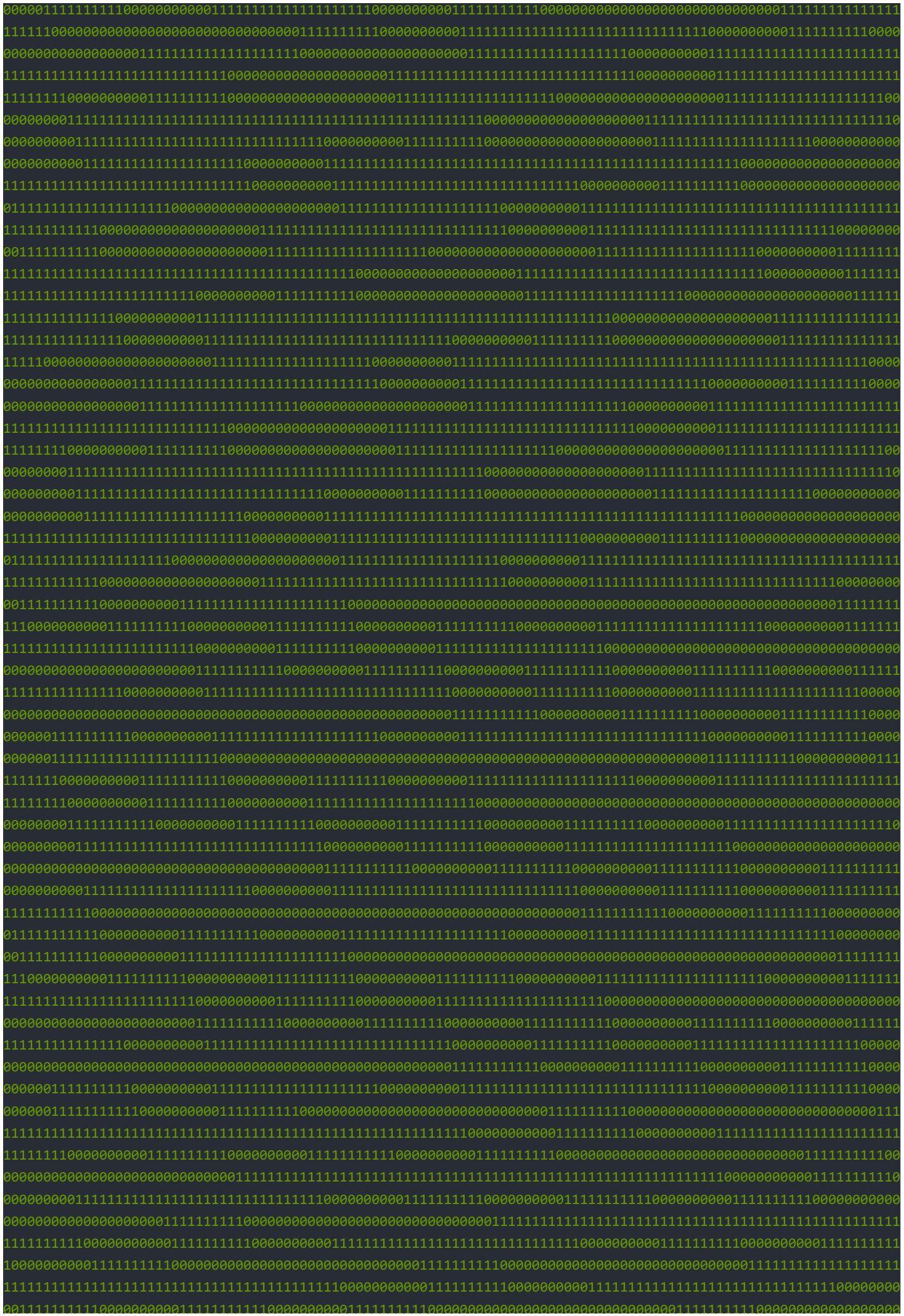


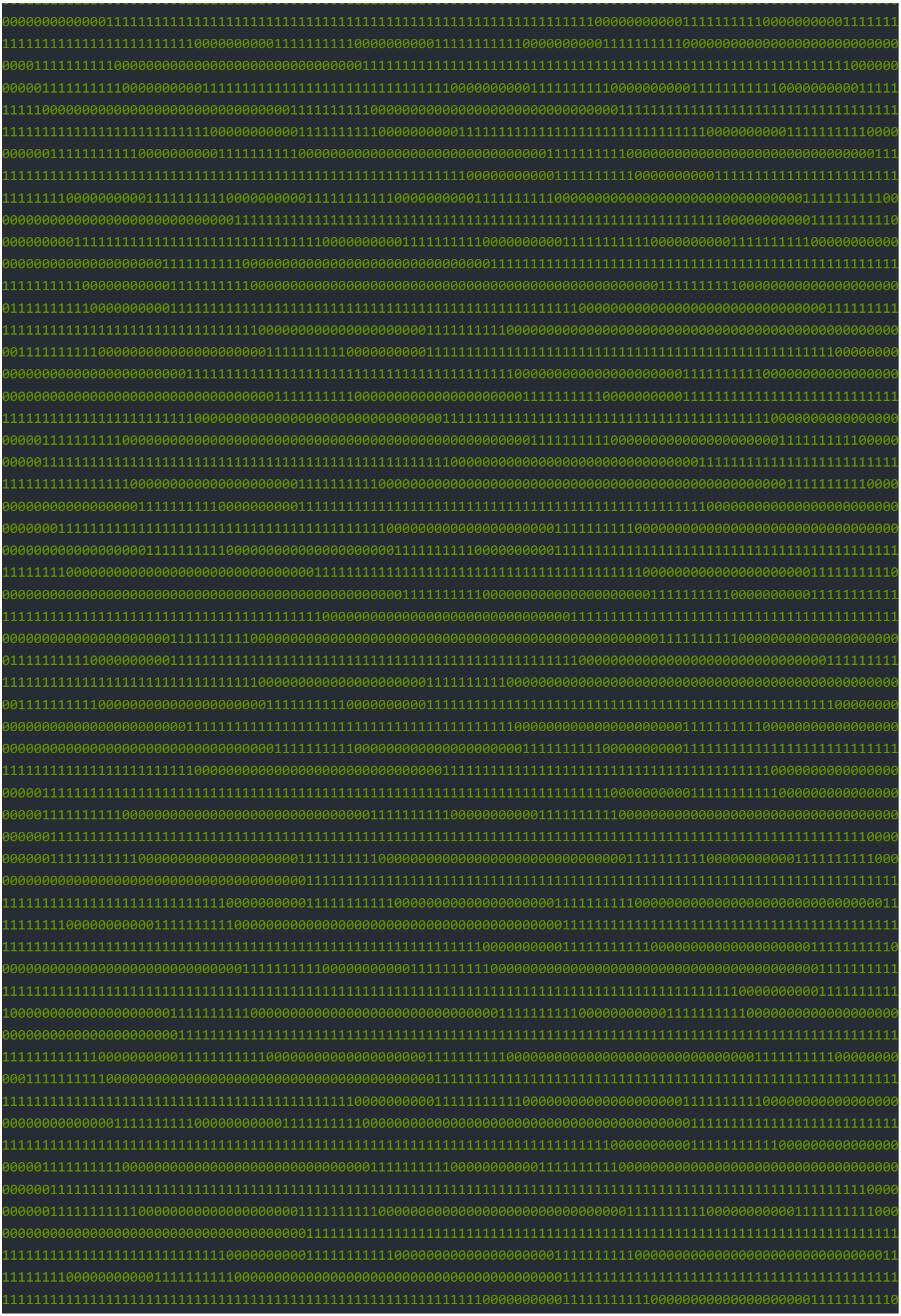












```
0000000000000000000000000000000011111111110000000000111111111100000000000000000000000000000000000000001111111111
11111111111111111111"
i = 0
for y in range (0,MAX):


    for x in range (0,MAX):


        if(str[i] == '1'):


            img.putpixel([x,y],(0, 0, 0))


        else:


            img.putpixel([x,y],(255,255,255))


        i = i+1
img.show()
img.save("flag.png")
```

然后这里需要注意

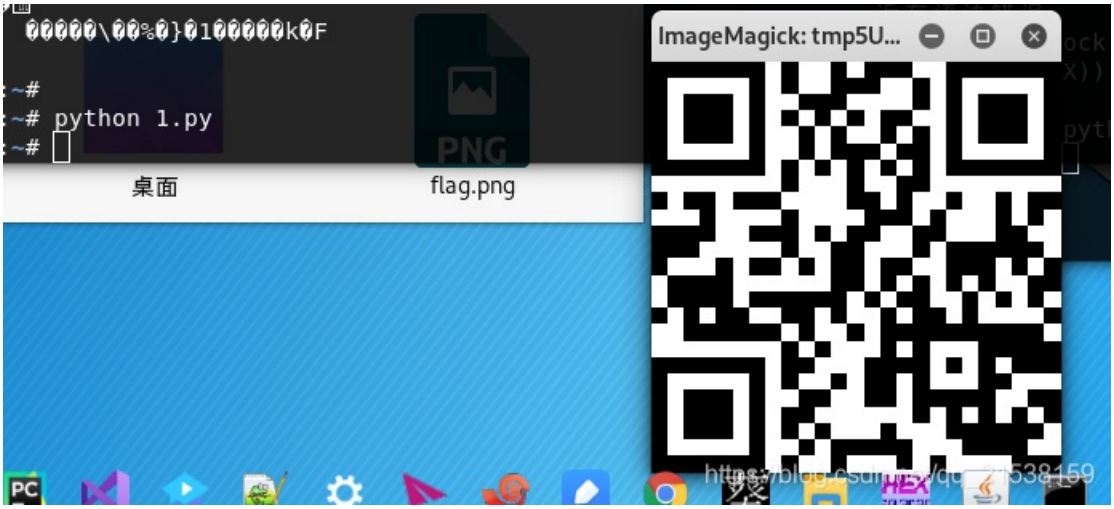
win下的PIL并不太容易装

而kali下集成了python环境，而且内置很多库

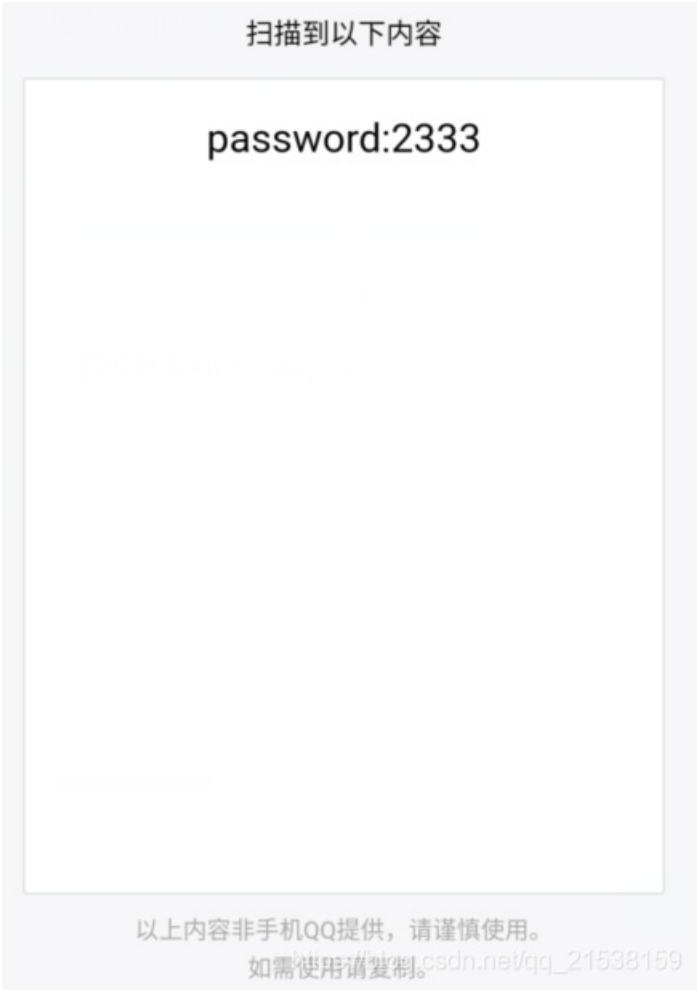
所以这里需要在kali下run

(这里需要感谢彦林小朋友的代码分享)

然后秒出

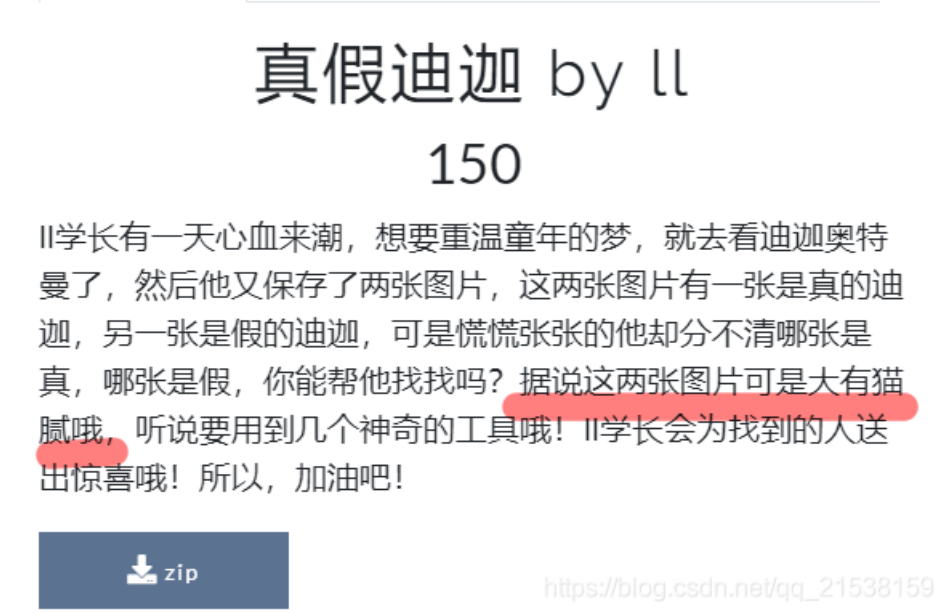


扫二维码后得到



好了，到此为止，迪迦1的戏份就结束了，为什么这样说呢。

其一，



其二 还记得foremost出来的原图嘛

我们来看一下几张图片的大小吧

迪迦一如下

迪迦二如下

foremost出来的原图

这里就很，明显了

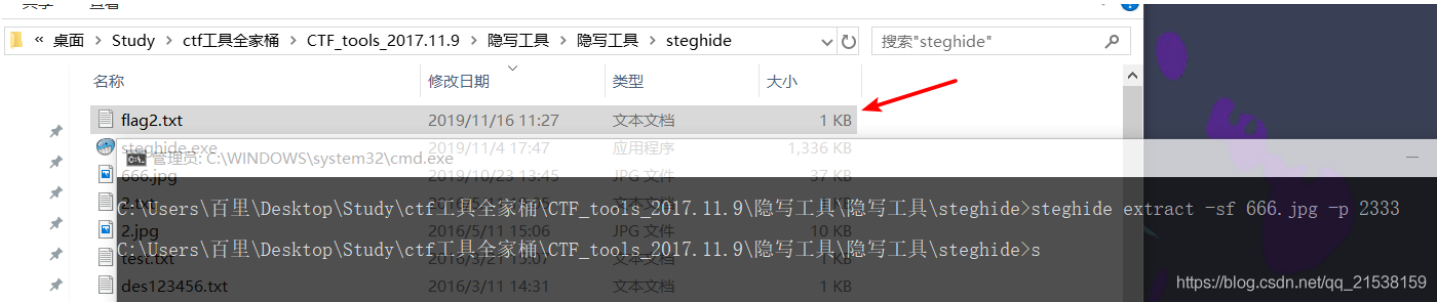
迪迦2也是有东西的
但是binwalk并没有看到别的东西。再结合刚解出来的flag1是一个密码
推断出这玩意因该是被加密的隐写，而不是简单的结合

这里就绕了很大的一个弯路

。。。。。。
先是stegsolve下研究了半天，未果
然后又走上了另一条弯路
以为是LSB加密隐写，然后又耽误了好长时间

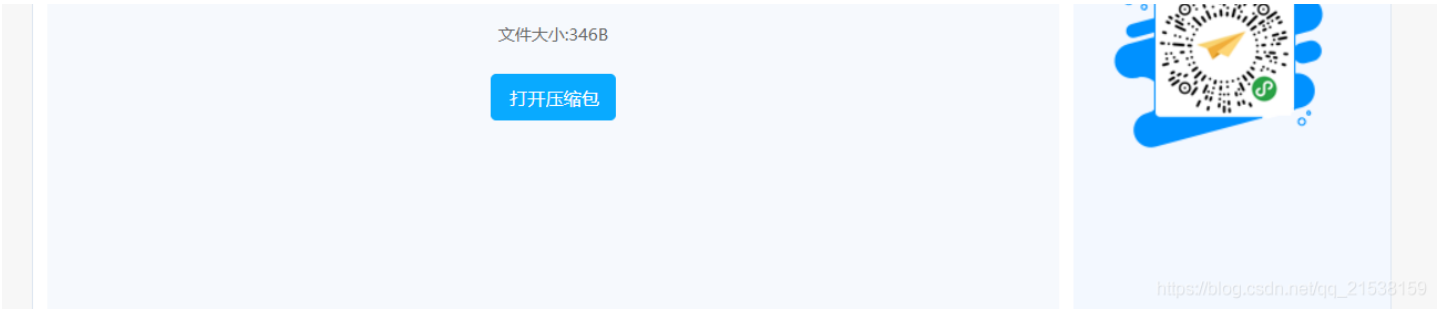
就是没想到用**Steghide**去试一下

然后这里



运行完后，在当前文件夹下跳出flag2.txt

然后就到了这里



诶，这个头像好熟悉啊

嘻嘻

然后下载解压打开

出现flag3.txt

打开进去

还是打下马吧

至此，本题解析完毕

总结如下

题目本身并不是很难，更多考查的是熟练各种工具对不同文件的分析，而这需要在长期刷题的一个过程中不断去提炼，总结，反思，然后进步。

最后致敬出题人