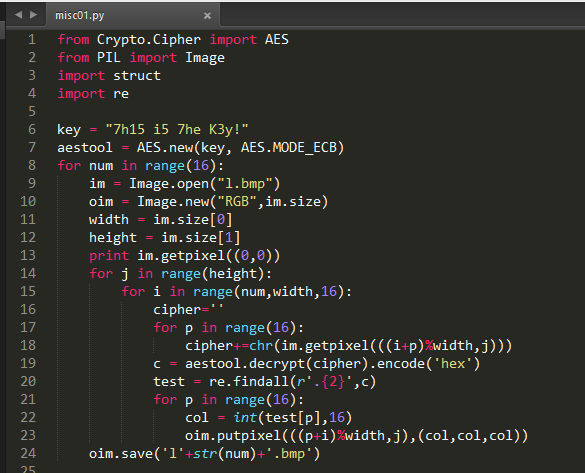
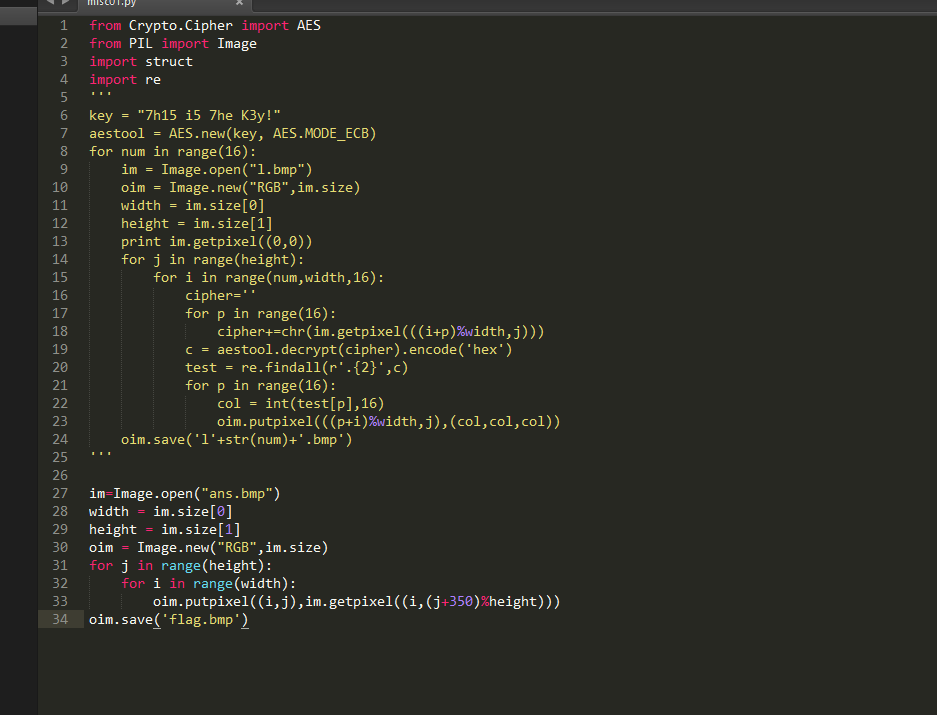
## 0x01 MISC01(250pt) The Truth That You Leave

图片的条纹很像是AES加密的结果 图片上还正好给出了16位的key

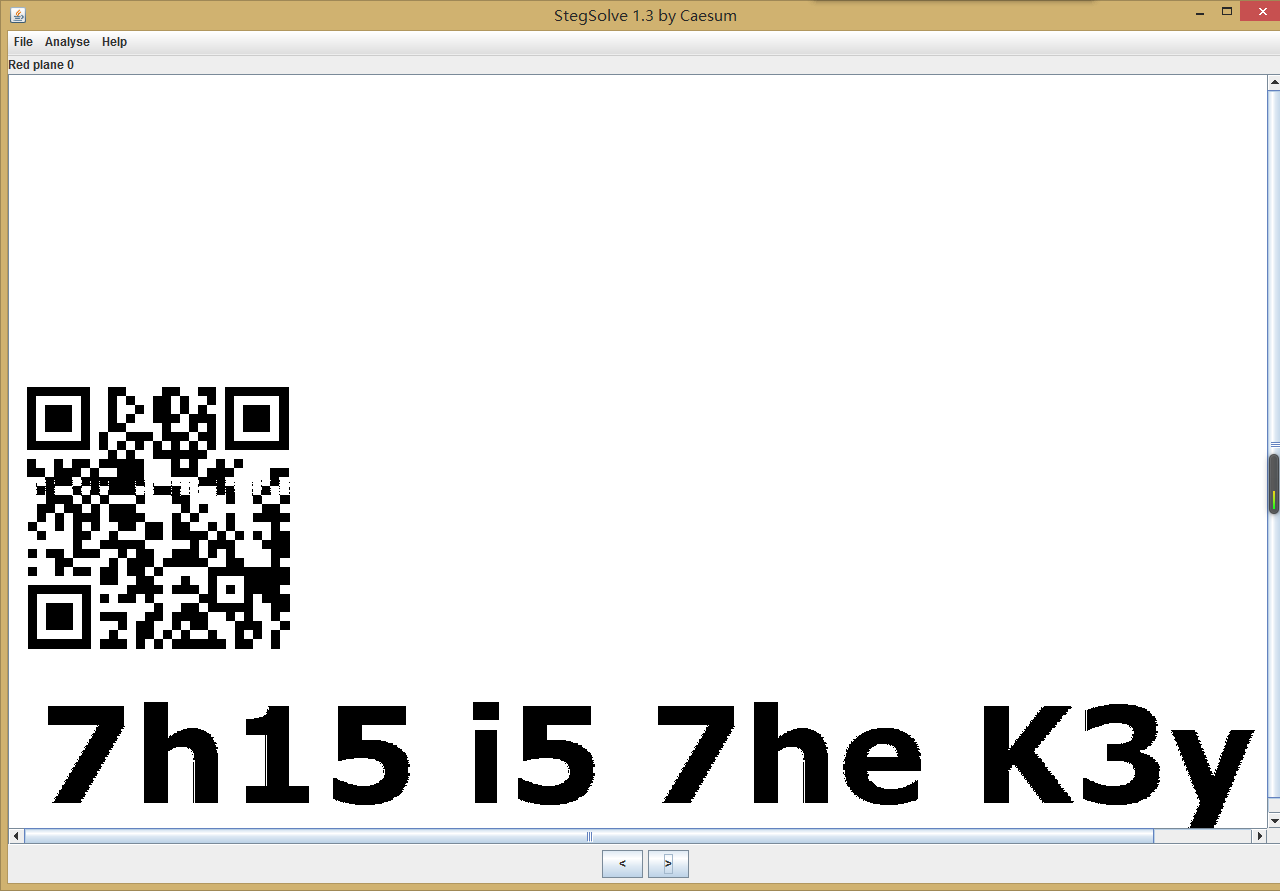
由于图片似乎是进行了一定的偏移操作，因此枚举偏移量进行解密



移动下图片，使得二维码能在图片中间。

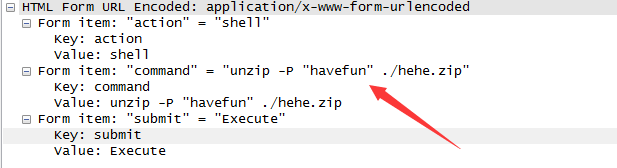


丢进StegSolve，在Red plane 0看到二维码，解码得到flag



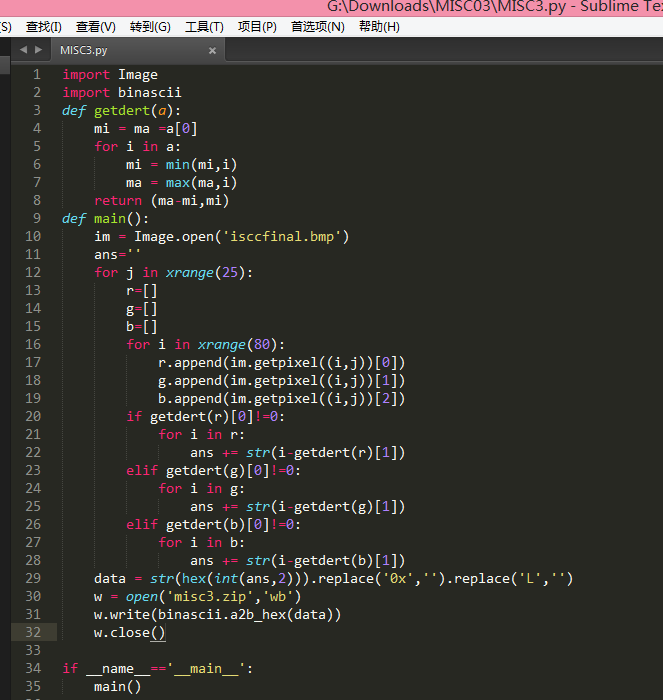
## 0x02 MISC02(300pt) Godlike

发现用户用一个php后门上传了一个hehe.zip的文件，抠出来解压得到flag



## 0x03 MISC03(300pt) 道之道

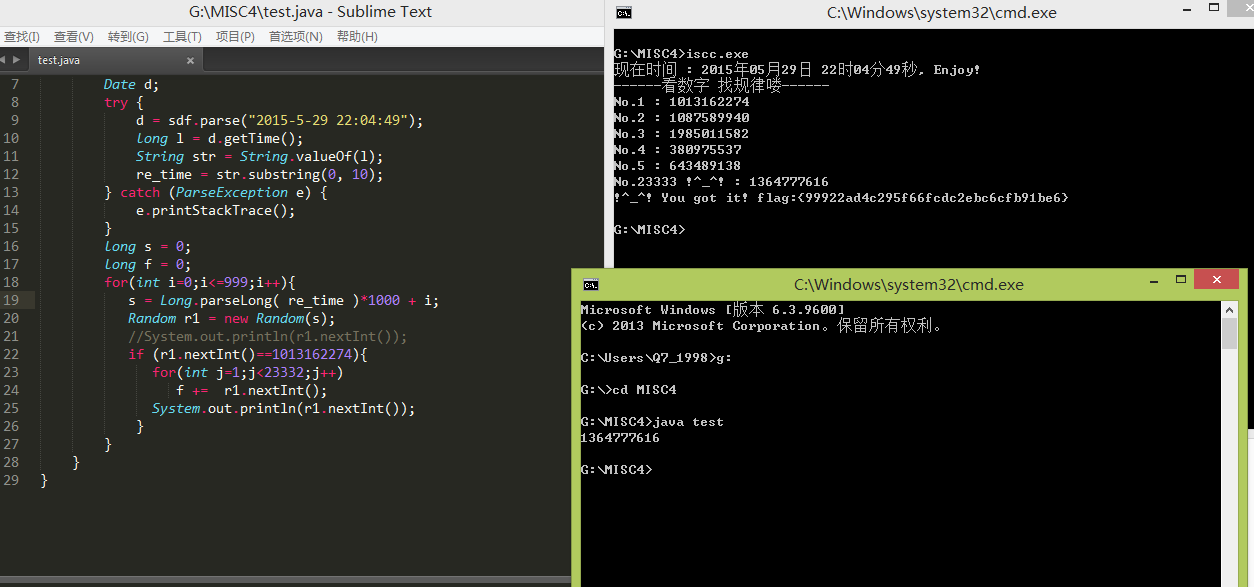
类似于LSB的一个隐写。



根据提示rot13对文件尾部字符串解码就是zip的解压密码，解压得到flag。

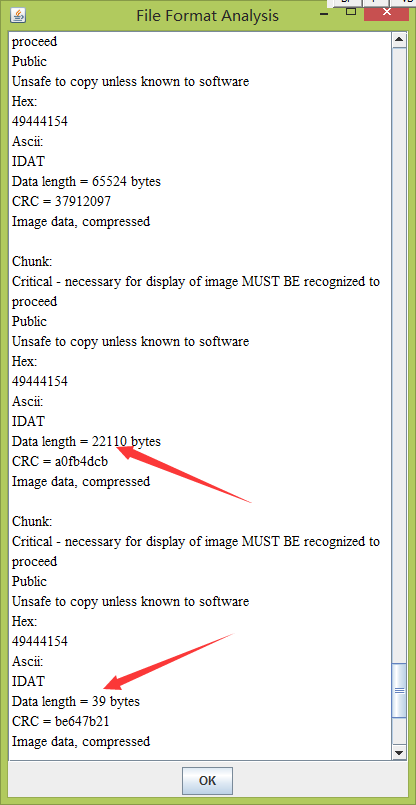
## 0x04 MISC04(350pt) 看序列，找规律。

看到JAVA和时间戳，猜测是java的随机数，写个程序爆破时间戳毫秒作为种子置随机数得到flag。



## 0x05 MISC05(350pt) 细节决定成败

打开文件发现有IHDR标识却是GIF的magic number，修改为PNG成功打开图片



看下IDAT发现最后一个IDAT块明显有问题。抠出后发现789C的zlib的magic number

解压得到flag。

