

ISCC2017 Misc write up附件题目文件

原创

椰树ii 于 2017-05-25 13:09:01 发布 2359 收藏 2

分类专栏: [ISCC](#) 文章标签: [ISCC2017 ISCC比赛 WP Misc write up](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_36512966/article/details/72724471

版权



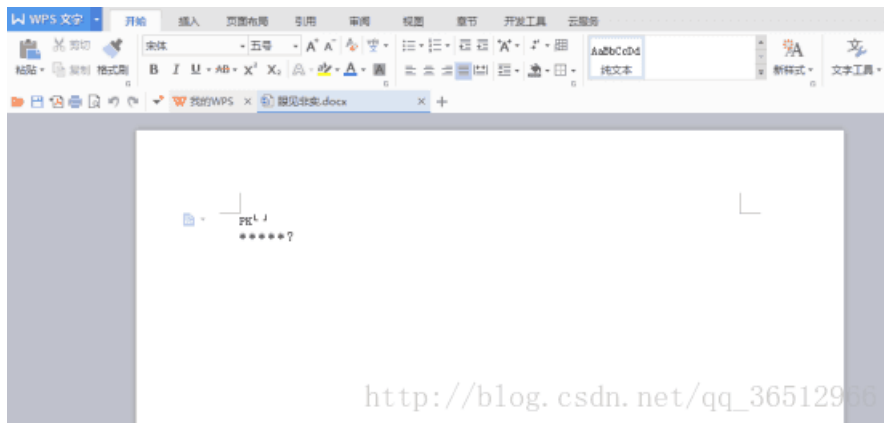
[ISCC 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏



打开附件是个.docx文档, 打开是乱码。



改后缀名为.zip

打开发现:





http://blog.csdn.net/qq_36512966



http://blog.csdn.net/qq_36512966

使用命令 (linux) openssl rsautl -decrypt -in key.txt -inkey test.key -out 1.txt



http://blog.csdn.net/qq_36512966

三三

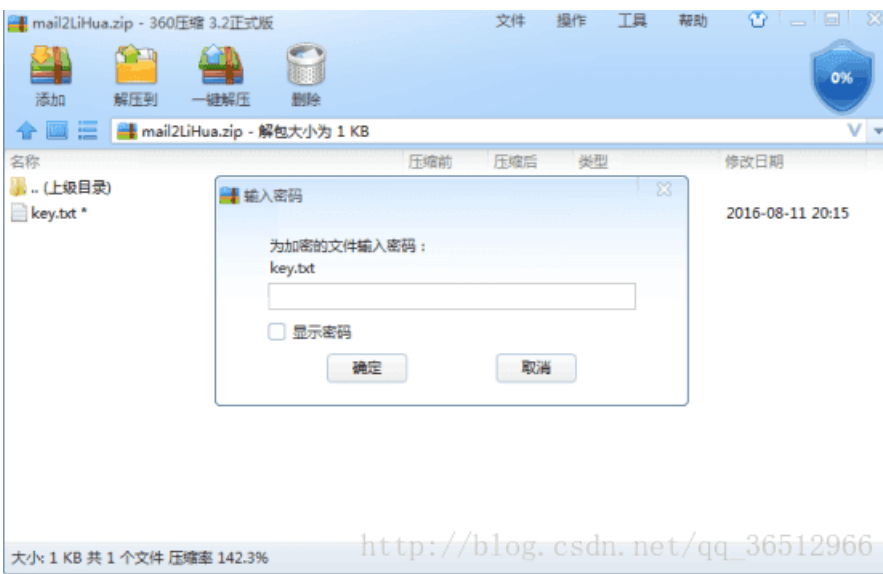


http://blog.csdn.net/qq_36512966

打开附件，发现是张图片，md5:1a4fb3fb5ee12307,在线查询md5发现根本查不到。



既然是图片，可能存在隐写，所以改后缀名试试。没错，确实存在一个.zip文件，但需要密码。



在winhex里看了下 不是伪加密。

那就是暴力破解了。

从题目：“没有任何特殊字符，请输入密码，记得署名哦”中获取信息。

大概下密码为：xxxxxxxLiHua具体x有多少位并不知道（其实这里有个技巧就是暴力破解压缩包密码一般在9位数以下，出题人不会让你破解密码好几天的。）

用木头字典生成自定义字典。

爆破之



Flag:



四

很普通的Disco

250

302 solves

普通的DISCO我们普通的插----

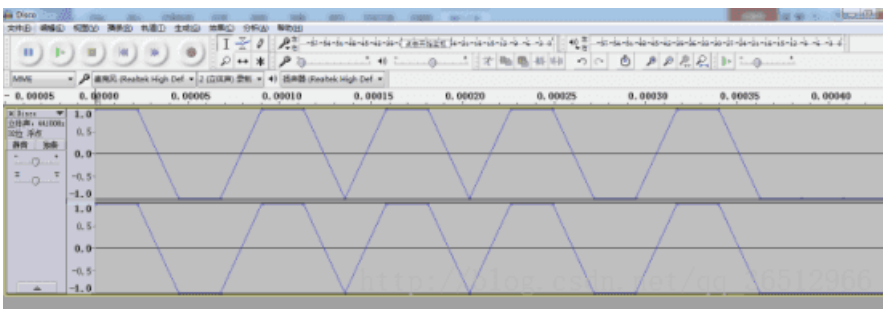
附件下载

Flag

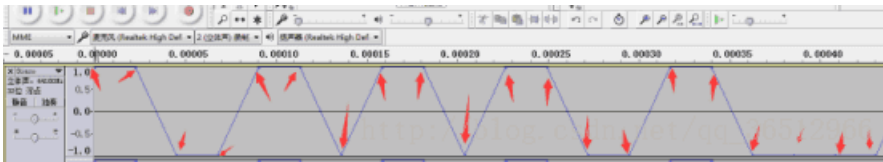
提交

http://blog.csdn.net/qq_36512966

音频文件，用Audacity打开，放大音频，发现一开始有一段地方有规律。



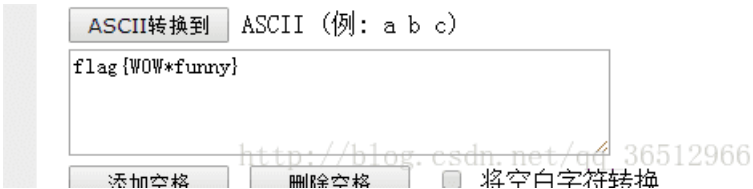
发现图像上边有点。



于是想到二进制01。上1下0。于是把图像转化为0和0得到二进制串。

1100110110110011000011100111111101110101110110000101011101010101100110111010111011101101

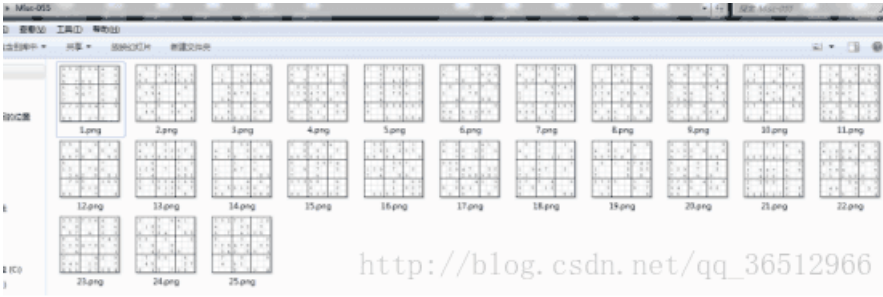
在线二进制转ascii码得：



五



打开附件



这里附上个脚本：

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-
import pytesseract
from PIL import Image, ImageDraw
def get_qr_list():
    qr_list = list()
    for a in range(5 * 9):
```

```

qr_list.append(list())

for b in range(5 * 9):
    qr_list[a].append(0)

for e in range(5):
    for f in range(5):
        fname = '%s.png' % (e * 5 + f + 1)

        img = Image.open(fname).convert('L')

        sx, sy, ex, ey, tx = 0, 0, 0, 0, 2
        for x in range(9):
            ty = 2
            tx += 1
            sx = x * 22 + tx + 1
            for y in range(9):
                ty += 1
                sy = y * 21 + ty + 1
                ex, ey = sx + 20, sy + 19

            img_temp = img.crop((sx, sy, ex, ey))

            code = pytesseract.image_to_string(img_temp, config="-psm 5")

            if code!="":
                qr_list[f * 9 + x][e * 9 + y] = 1
                print(qr_list[f * 9 + x][e * 9 + y], (x, y), (sx, sy, ex, ey), (e, f, x, y))

return qr_list

def get_qr_image(qr_list):
    img = Image.new('L', (10 * 47, 10 * 47), (255))

```

```

draw = ImageDraw.Draw(img)

for e in range(5 * 9):
    for f in range(5 * 9):
        if qr_list[f][e]:
            draw.rectangle(((e + 1) * 10, (f + 1) * 10, (e + 2) * 10, (f + 2) * 10), fill=(0))

        print(qr_list[f][e], ' ', end="")

    print()

img.save('flag.png')

if __name__ == '__main__':
    get_qr_image(get_qr_list())

```

在数独文件下运行该脚本（先把数独文件定位好，不懂怎么定位的自行百度二维码定位点知识，然后在运行脚本），得到个二维码，扫出的结果为：

Vm0xd1NtUXlWa1pPVldoVFIUSINjRIJVGtOamJGWnlWMjFHMUxv1ZqTldNakZIwVcxS1lxTnNhRmhoTVZwe\



Base64多次解密得：flag{y0ud1any1s1}

ISCC2017-Misc-题目下载:<https://pan.baidu.com/s/1geVZM9t>