i春秋公益赛WriteUp-MISC套娃

原创

L.o.W 于 2020-02-24 17:31:22 发布 2559 收藏 2

分类专栏： CTF WriteUp 文章标签： 信息安全 zip

本文链接：https://blog.csdn.net/weixin_44145820/article/details/104479837

2020.3.4：更新了选择明文攻击部分

这道MISC考察的是压缩包解密和隐写

第一关：Ook编码

```
//1.剧情.txt
1小童鞋也想变强，他的老师告诉他如果能去西天取到真经 ，那成长速度堪比吃一盒仙丹。

小童鞋谨遵老师教诲，终于准备前去西天。

老师说拿到真经借我看看，小童鞋说：
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook. Ook! Ook! Ook! Ook. Ook! Ook!
Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook?
Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook?
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook?
Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
```

```
Ook. Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook! Ook.
Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook.
Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook. Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook!
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook?
Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook.
Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook.
Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook. Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook!
Ook. Ook? Ook! Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.
Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook!
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!
Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook.
```

直接在线解码即可，网址：https://www.splitbrain.org/services/ook
结果是压缩包2的解压密码

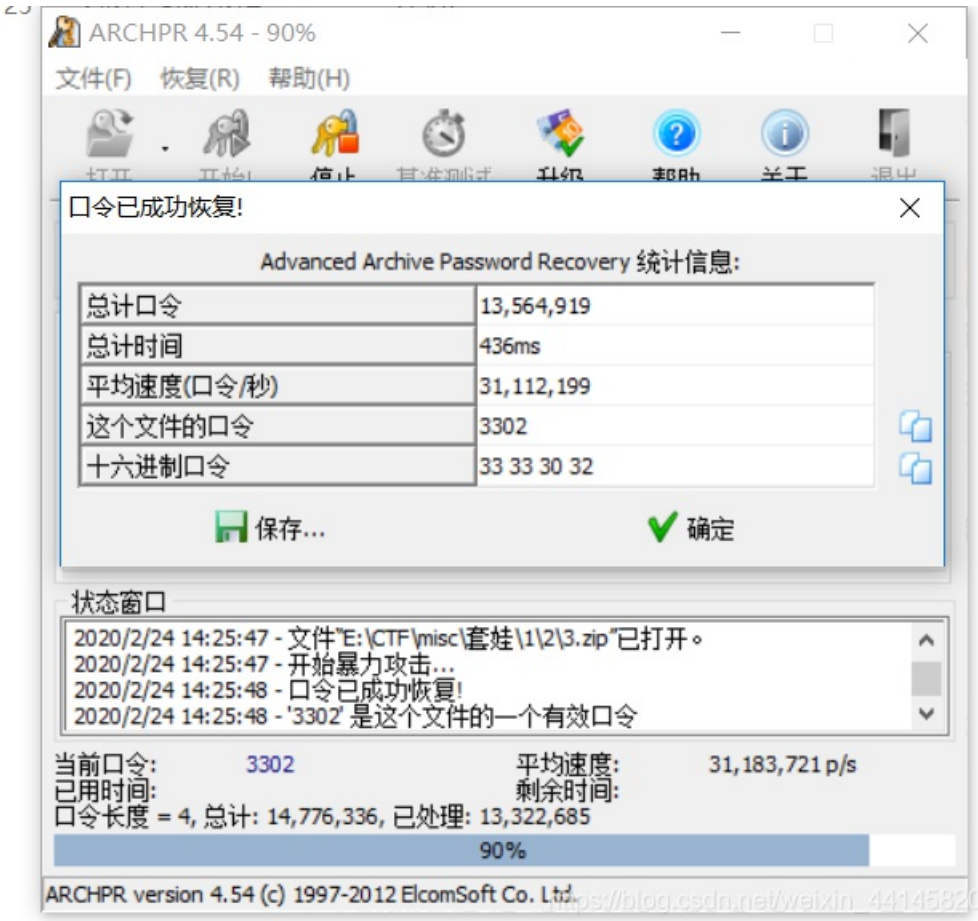
> dcaf03aa88d038686c5e8067a7a45ff8

第二关：爆破

```
//2.剧情.txt
2.是吧，套娃都是简单题~

哎呀 怎么不按剧情发展，走的匆忙，老师没有给你准备白龙马 路程这么远 先捡个路边ofo小黄车骑吧
```

第二关并没有什么提示，图片中有一个二维码，不过并没有什么用…

直接爆破压缩包



得到密码3302

第三关：伪加密

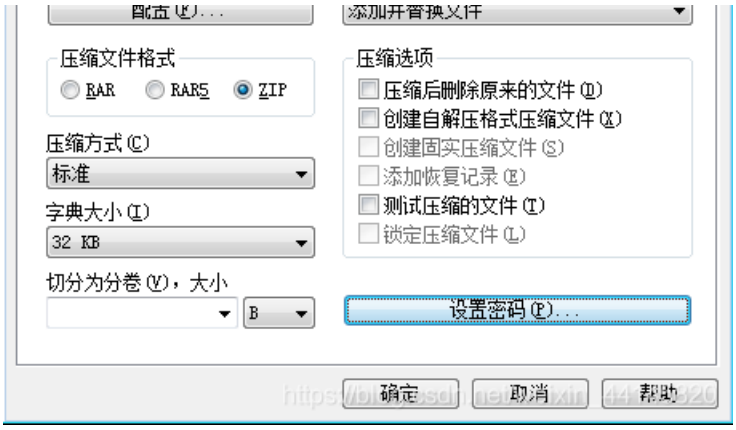
```
//3.剧情.txt
3.恭喜你骑上了小黄车（不嫌累嘛

边上那个膜拜电单车不香嘛？

（强制换乘膜拜有气嘛？hhh

emmm 怎么打开他呢，好像也没锁好？虚张声势？纸糊的？
```

虚张声势，那可能是伪加密
360压缩可以直接解压

第四关：选择明文攻击

```
//4.剧情.txt
4.摩拜要出管理范围了，路边有个美团单车 外观看起来好像没啥区别，骑上试试吧。
```

题目给了提示

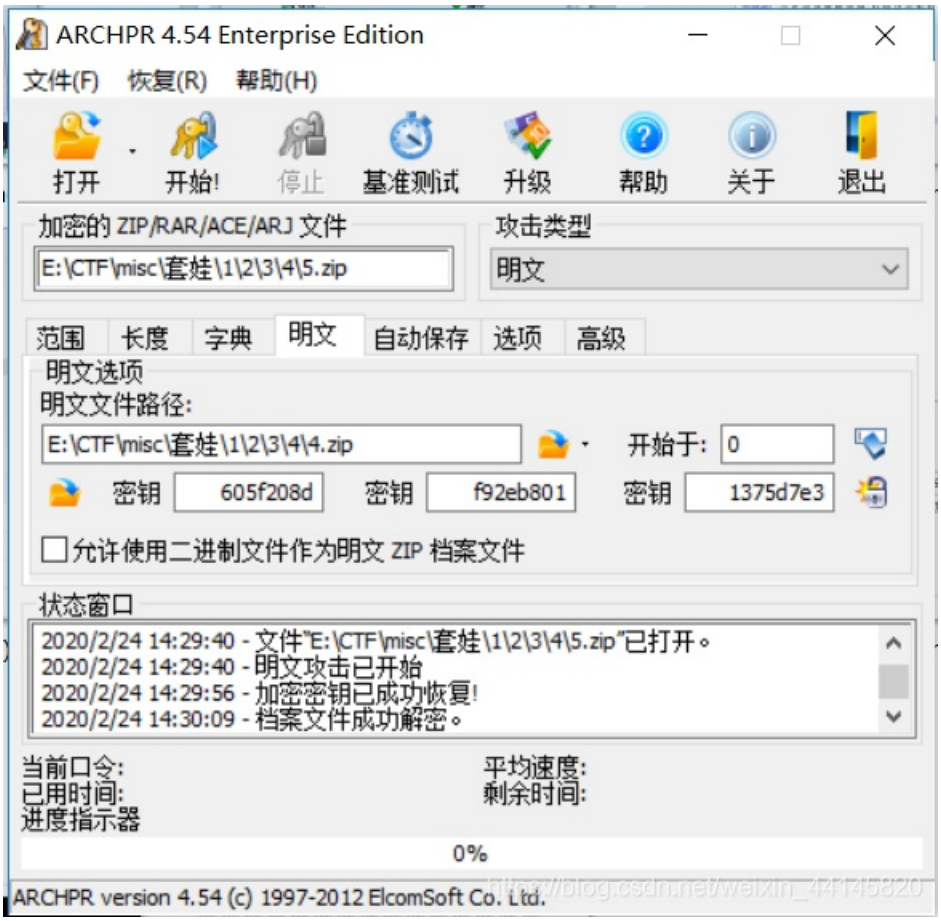


打开5.zip,发现也有4.jpg

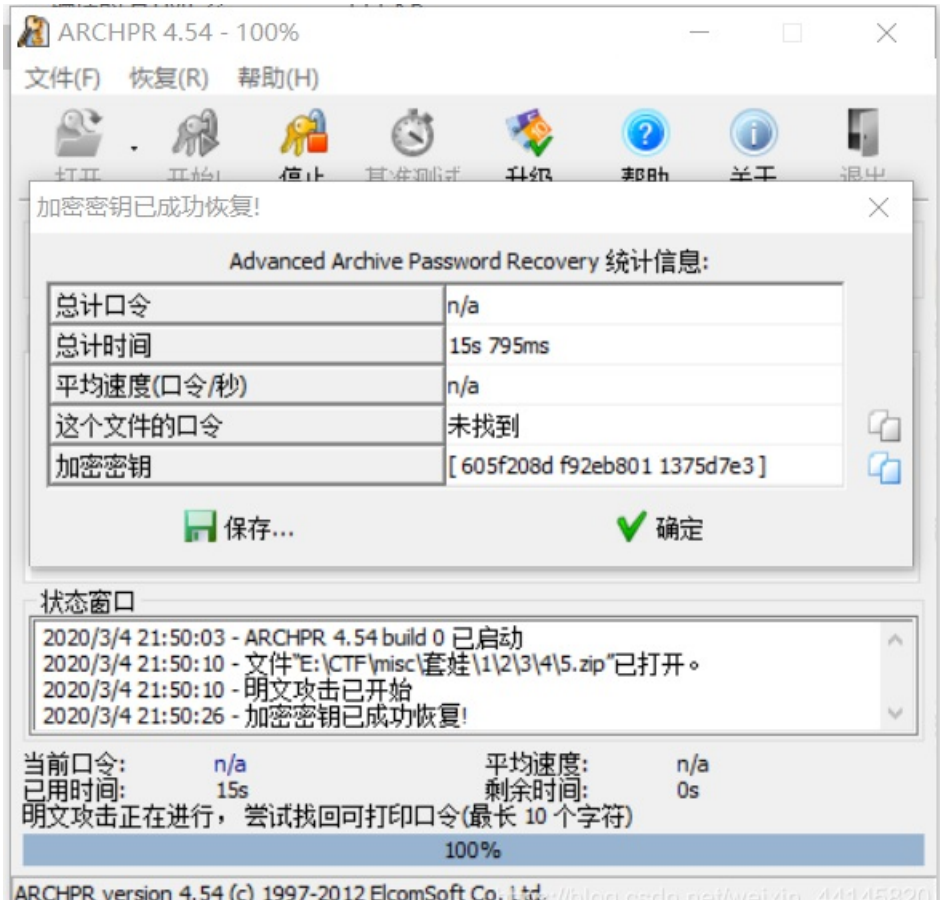
使用ARCHPR进行选择明文攻击

首先，把4中的4.jpg用winRAR压缩为4.zip

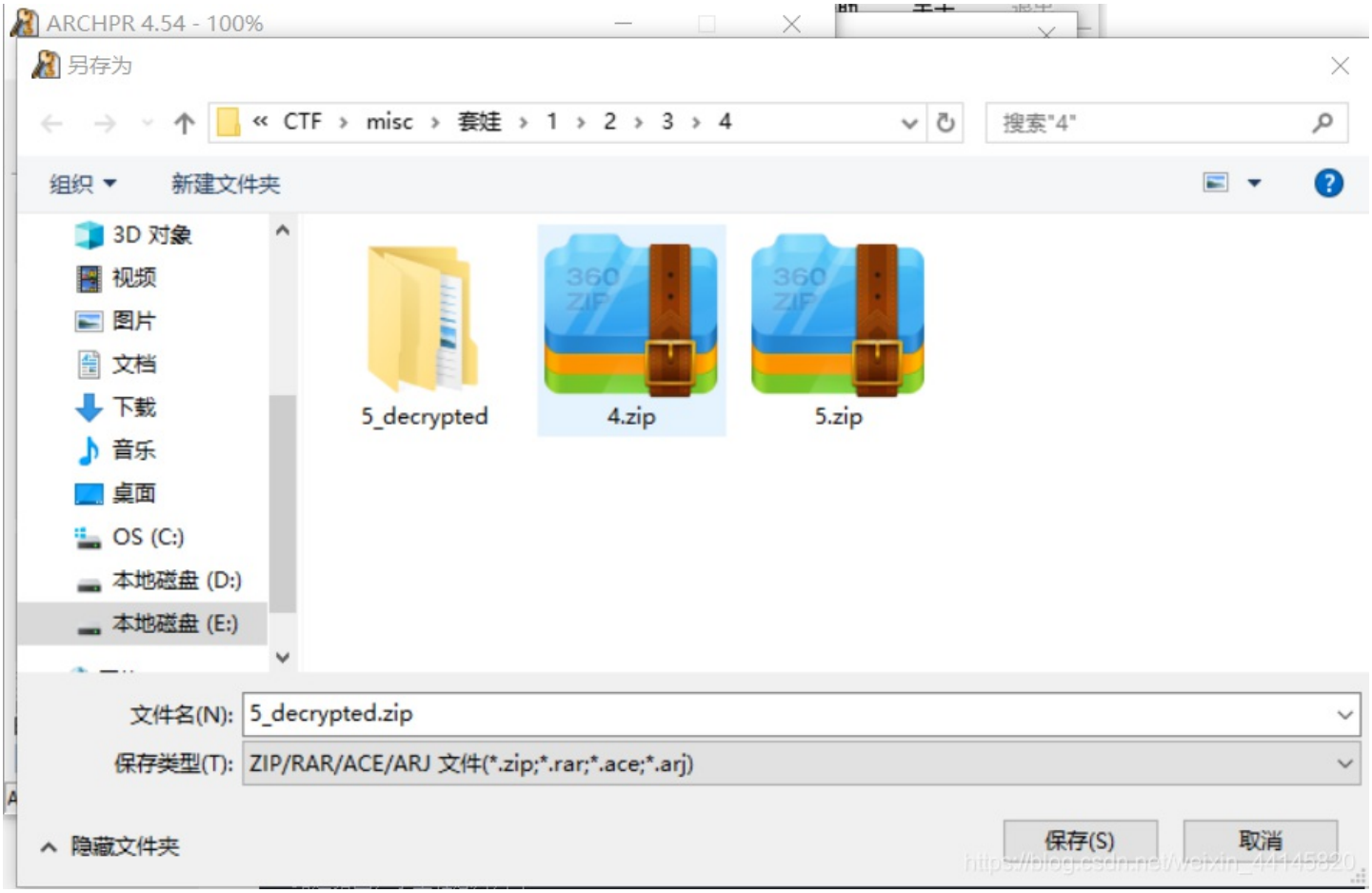
打开ARCHPR，选择明文攻击，明文文件选择刚才生成的4.zip，如下图



这里ARCHPR并不能还原出密码，不过能得到解密之后的压缩包

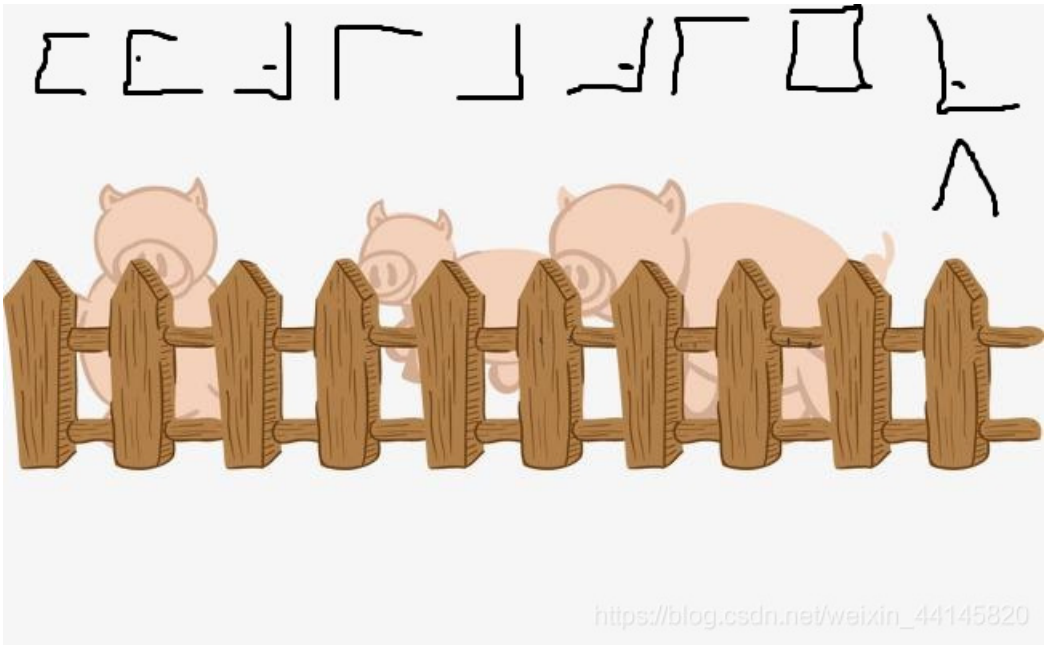


下面是解密出的文件

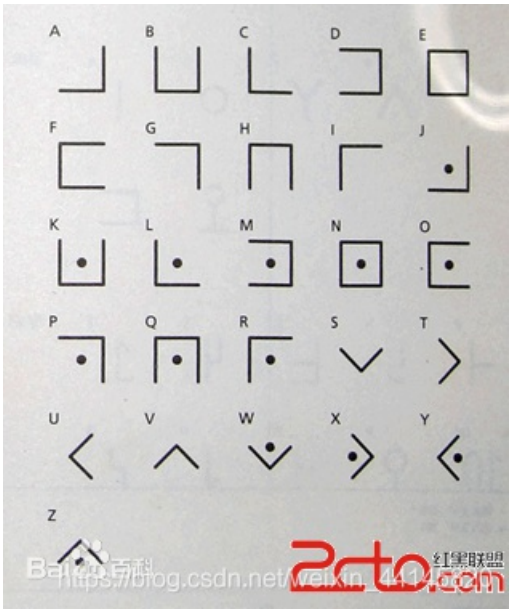


第五关：猪圈密码

```
//5.剧情.txt
5.路过猪圈，小童鞋想开开荤
```



根据题目提示为猪圈密码：



结果是：fojiajielv

第六关：与佛论禅

```
//6.剧情.txt
6.继续往前走，见到有佛家僧人讲经
```

使用在线网站解密，注意前面要加上**如是我闻**（不知道为什么加佛曰解不出来…）

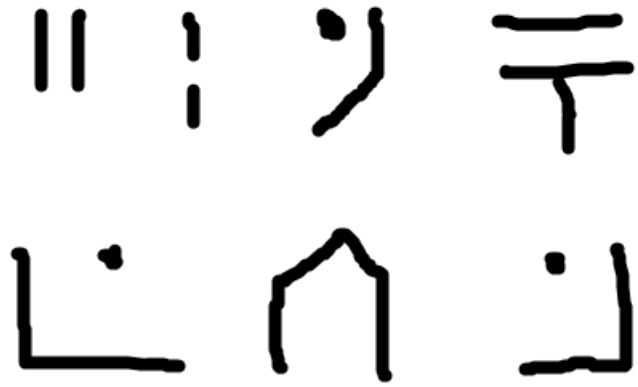
```
如是我闻：曰罰醢缽夢冥無缽特冥。提罰不是怯羯俱孕帝穆罰遠奢大勝俱諸冥滅得滅怯怖波栗俱搏姪漫俱上吶無尼尼吶喝俱恐
```

结果：amtf12345

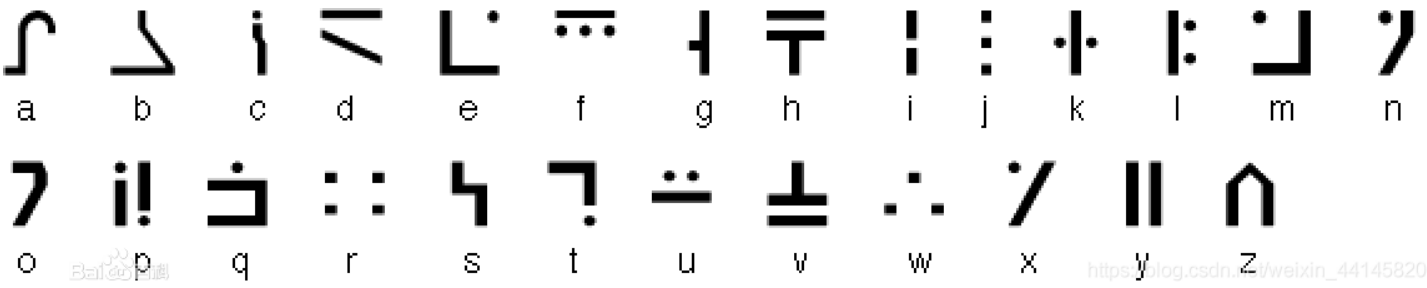
第七关：标准银河字母

```
//7.剧情.txt
7.进塔一看，4条腿的桌子上还有个啥台子？咋在往外冒字
```

7.png↓



标准银河字母



结果：yinhezm

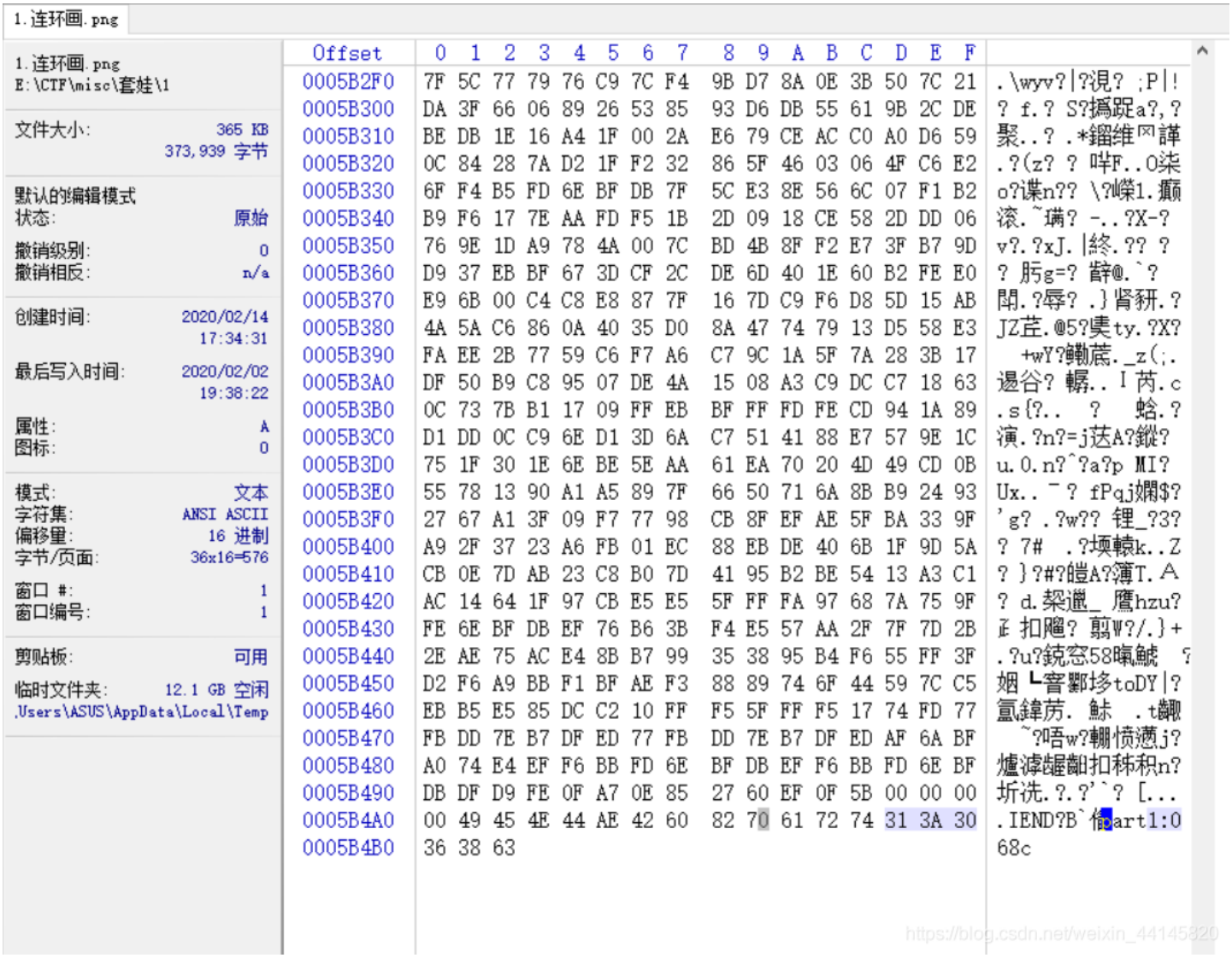
第八关：各种隐写

```
//8.剧情.txt



8.原来，真经就在塔顶，走到顶，两位存储尊者向你索要人事一些<既然出门匆忙没带经文 不如把一路上得到的战利品(共32位)交出来吧

!
```

看来之前的压缩包里还隐藏了第八关的密码…
只能重新回去看了

1. Winhex查看图片

藏在1.连环画.png图片的末尾：part1:068c

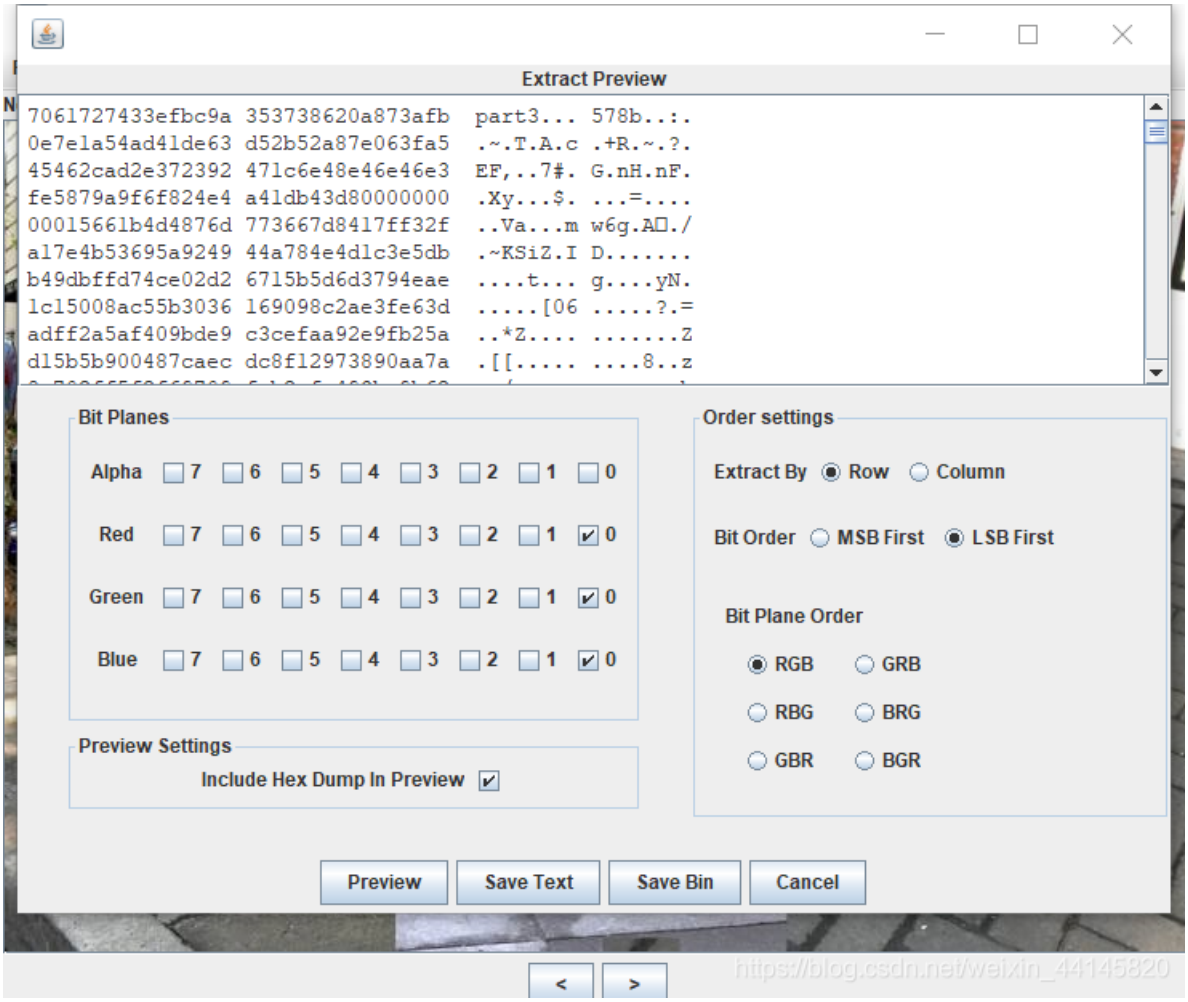


2.图片信息

右键打开2.连环画.png的属性，part2:555b

3.LSB隐写

用Stegsolve打开3.连环画.png，
Analyse->Data Extract
得到part3:578b



4.修改图片高度

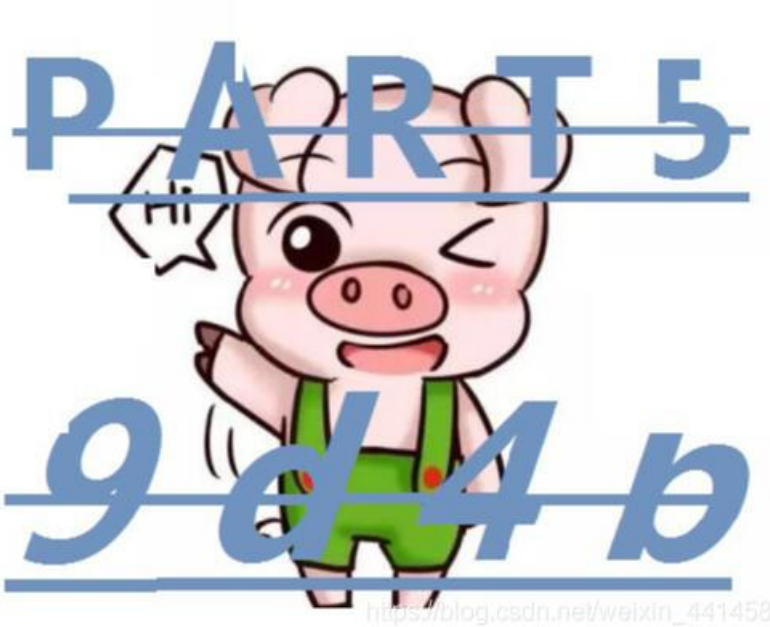
第四个给了一张截图，大小是1080 * 2069
而手机截图大小一般是1080 * 2310
修改高度得到part4:0eae

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	塒NG.....IHDR
00000010	00	00	04	38	00	00	09	06	08	06	00	00	00	39	8E	1A	...8.....9?
00000020	D4	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	?...sRGB.锑.?..
00000030	00	04	67	41	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	..gAMA..? .?a...
00000040	00	09	70	48	59	73	00	00	0E	C4	00	00	0E	C4	01	95	..pHYs...?...?.?

这里还有一个小技巧，如果图片高度被修改过，Kali Linux是打不开的

5.拼图

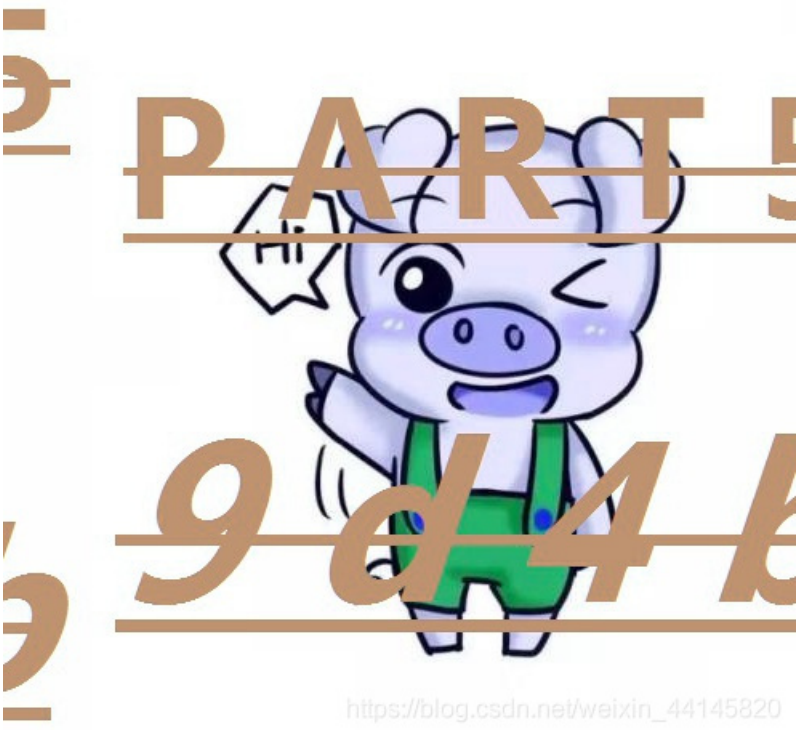
第五关的连环画全是碎片，拼完就是密码
part5:9d4b



经大佬指点，可以用gaps自动拼图，用法如下

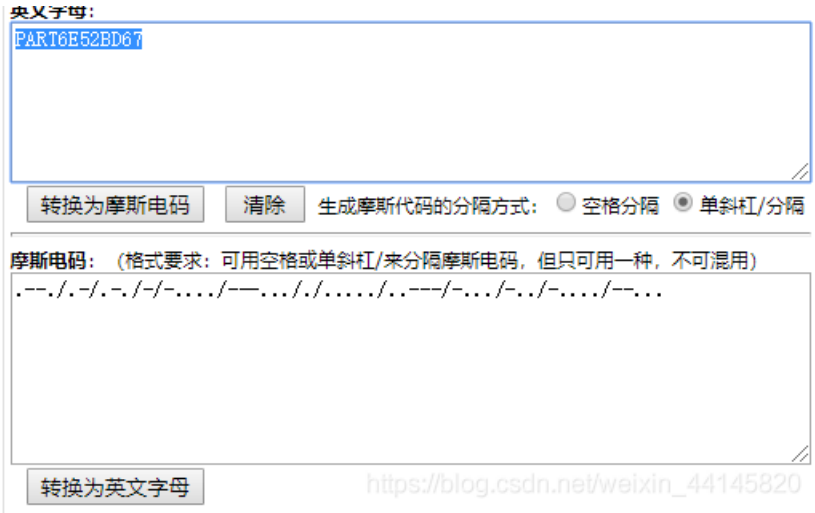
> 首先把81张图片合成
> montage *.png -tile 9x9 -geometry +0+0 flag.png
> 然后gaps就能自动拼图了
> gaps --image=flag.png --size=55 --save

gaps拼图效果如下：



6.摩斯密码

在6.连环画.png的末尾发现一串摩斯密码，
在线解密得到PART6:e52bd67
http://www.zhongguosou.com/zonghe/moErSiCodeConverter.aspx



7.Gif隐写

Gif隐写一般是是把gif的每一帧提取出来拼接在一起
不过这题是时间隐写··

> 查看时间
> identify -verbose 7连环画.gif |grep Delay
> 导出时间
> identify -format “%T” 7连环画.gif

得到
102020201010101010202010101010201020202010102010102020201020101010102020102020201010202020102010101
0202010202010101020201010102010102020102010201010202010202010101020201010102010
然后把10转化为0,20转为1，脚本如下

```
s = "1020202010101010102020101010102010202020101020101020202010201010101020201020202010102020201020101010202020102
02010101020201010102010102020102010201010202010202010101020201010102010"
s = s.replace("10", "0")
s = s.replace('20', '1')
print s
```

得到01串：01110000011000010111001001110100001101110011101000110110001100010011010100110110001100 10
转化为ASCII码：
part7:61562

至此，32位密码已经收集完毕

> 068c555b578b0eae9d4be52bd6761562

第九关：NTFS数据流隐写

```
//9.剧情.txt

9.取到经文 原路返回，龟丞相一不高兴，小童鞋掉进水里，出水一看，NT和FA给的经文是空白的？？
```

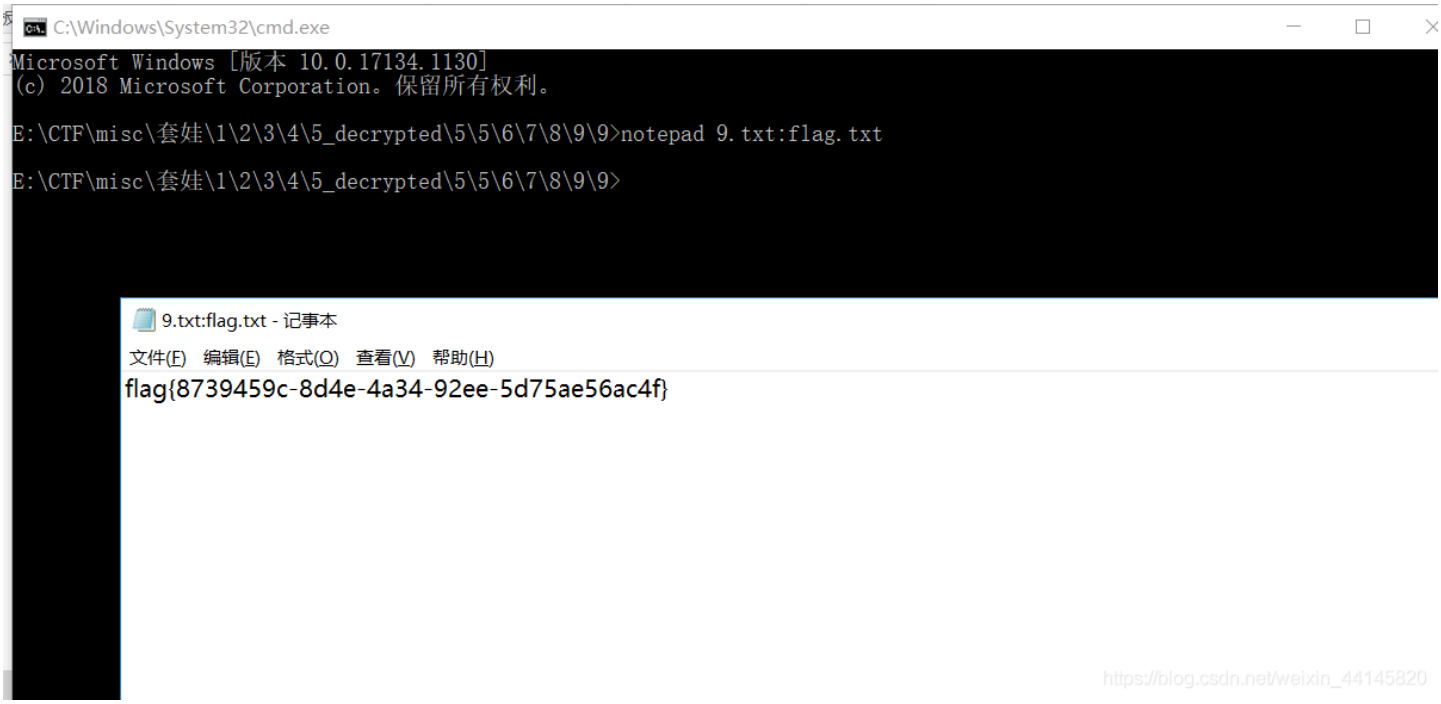
使用lads.exe查看一下：

> lads.exe path /S

```
Scanning directory E:\CTF\misc\套娃\1\2\3\4\5_decrypted\5\5\6\7\8\9\9\ with subdirectories

      size  ADS in file
----------  ---------------------------------
        42  E:\CTF\misc\套娃\1\2\3\4\5_decrypted\5\5\6\7\8\9\9\9.txt:flag.txt

        42 bytes in 1 ADS listed
```

然后用记事本打开,得到flag

> notepad 9.txt:flag.txt



更多CTF在线工具网站见：CTF Crypto/MISC 在线工具网站
