

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](#)

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/weixin_44145820/article/details/104479837

版权



[CTF WriteUp 专栏收录该内容](#)

9 篇文章 0 订阅

订阅专栏

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!

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

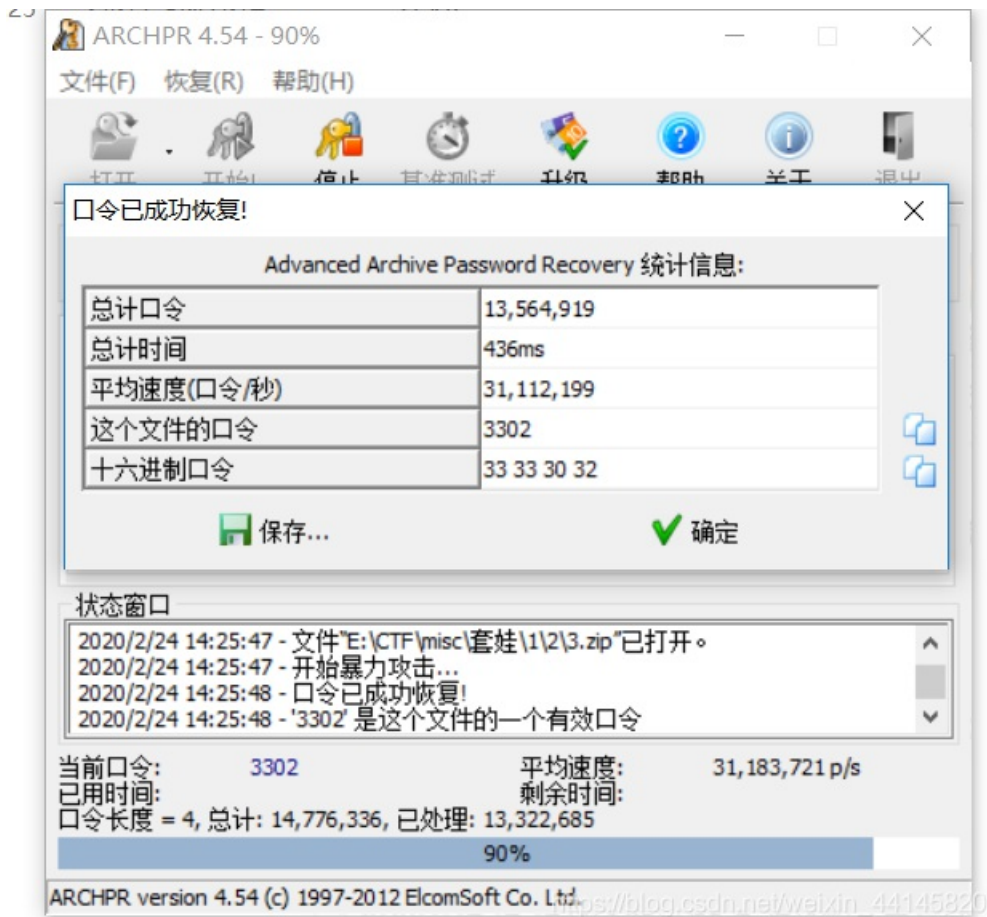
dcaf03aa88d038686c5e8067a7a45ff8

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



虚张声势，那可能是伪加密

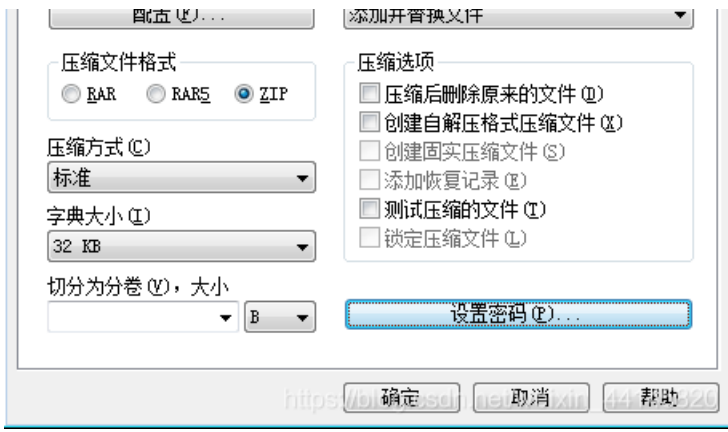
360压缩可以直接解压

第四关：选择明文攻击



题目给了提示





打开5.zip,发现也有4.jpg

5.zip (评估版本)

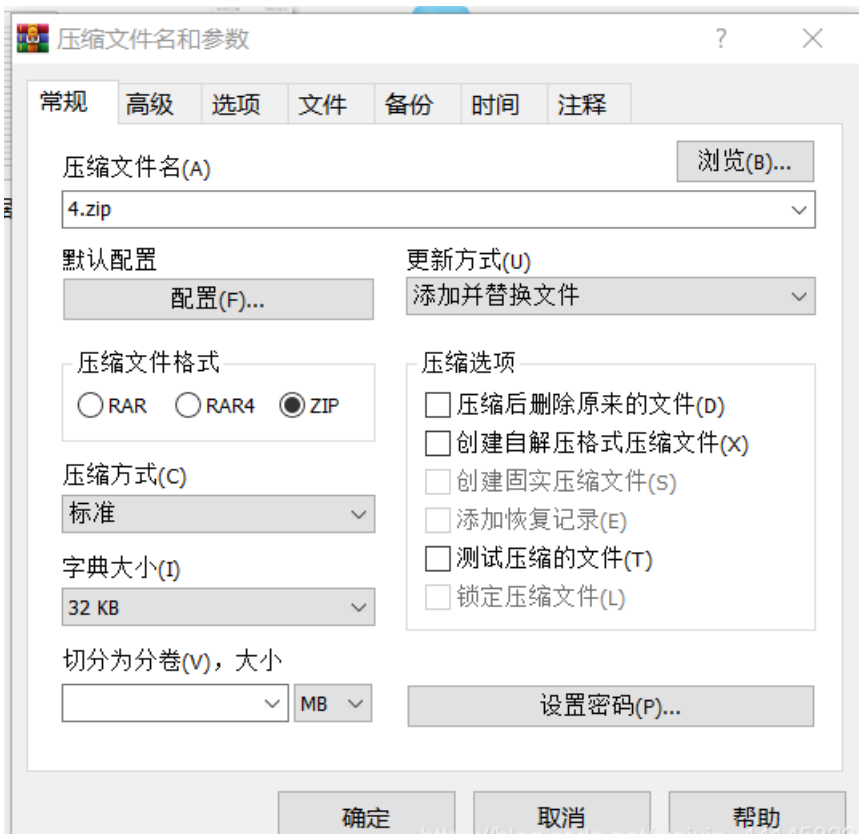
文件(E) 命令(C) 工具(S) 收藏夹(O) 选项(N) 帮助(H)



https://blog.csdn.net/weixin_44145820

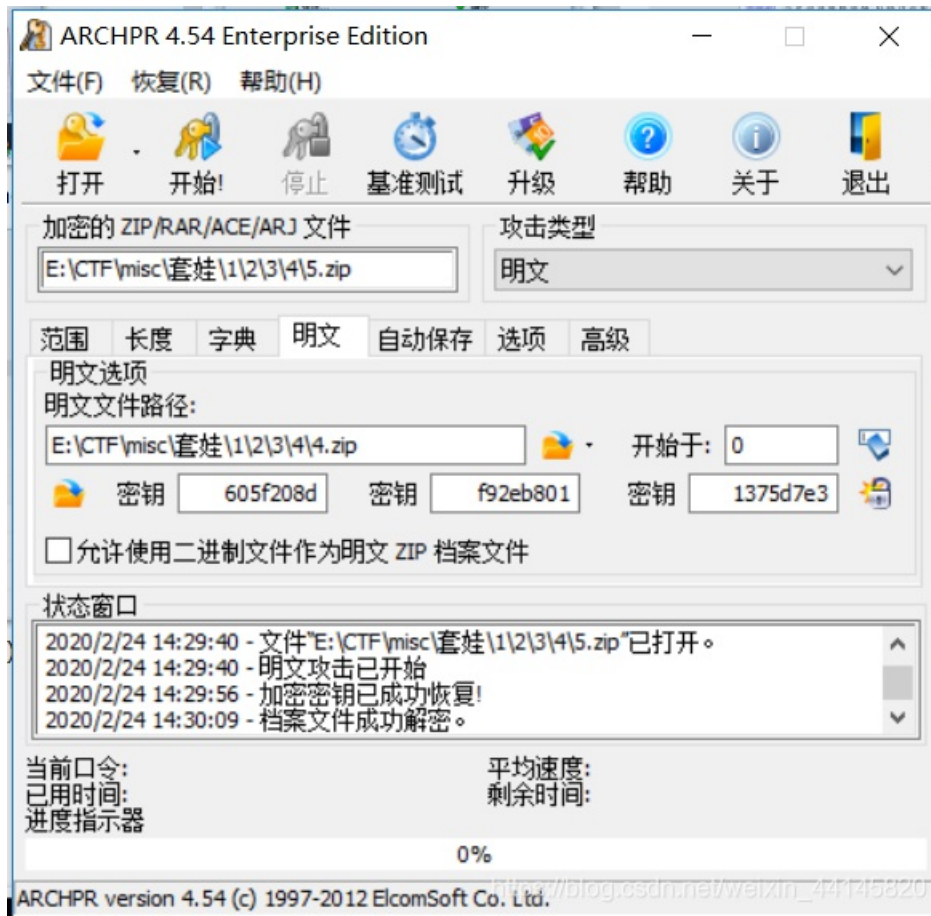
使用ARCHPR进行选择明文攻击

首先,把4中的4.jpg用winRAR压缩为4.zip

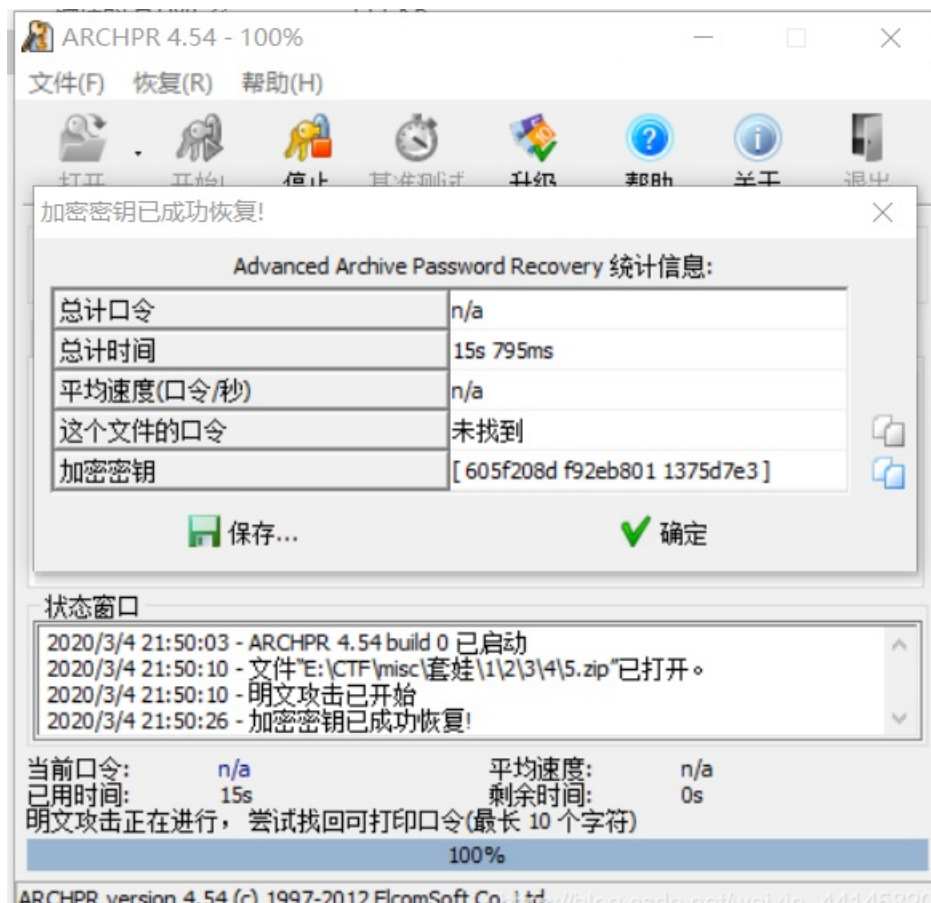


https://blog.csdn.net/weixin_44145820

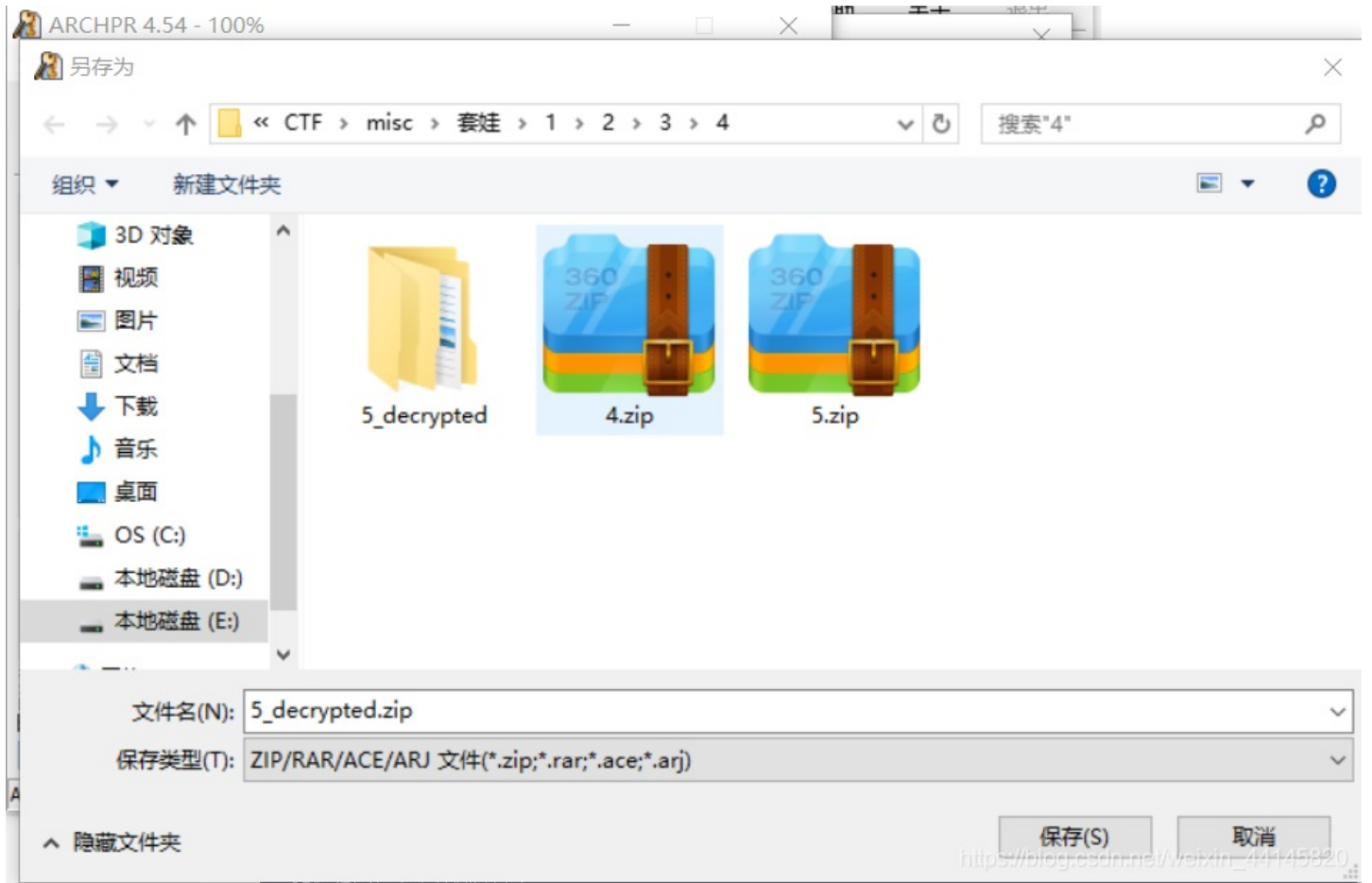
打开ARCHPR，选择明文攻击，明文文件选择刚才生成的4.zip，如下图



这里ARCHPR并不能还原出密码，不过能得到解密之后的压缩包

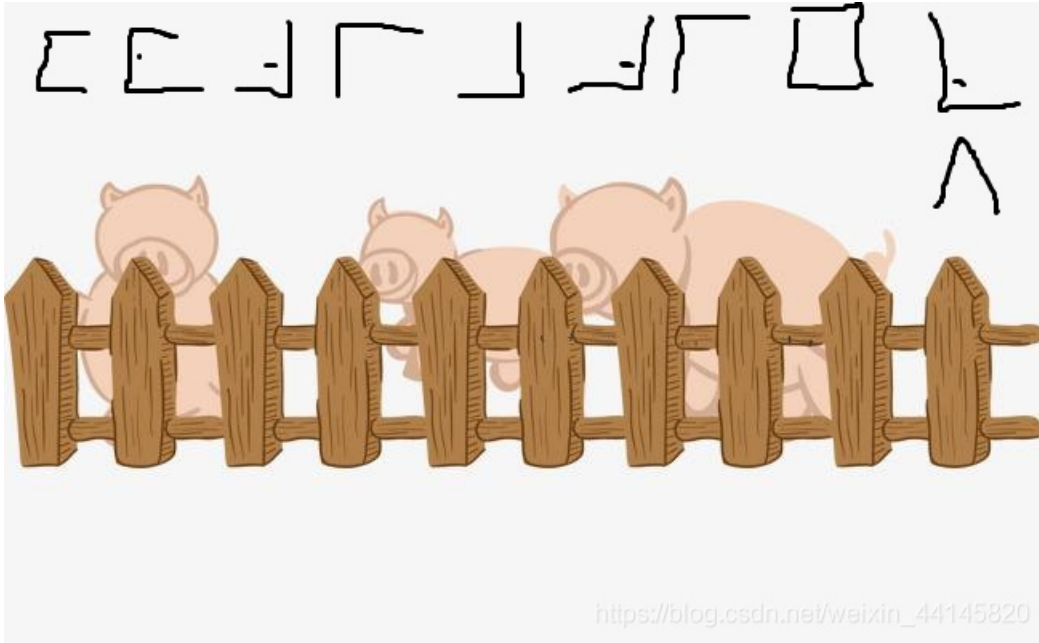


下面是解密出的文件

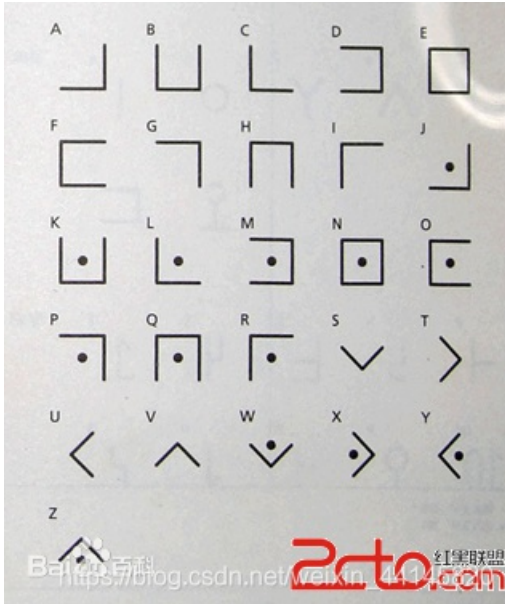


第五关：猪圈密码

```
//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：fojjajielv

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： 曰罰醢鉢夢冥無鉢特冥。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耨姪漫俱上呐無尼尼呐喝俱恐

结果: amtf12345

与佛论禅

pass = amtf12345

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

菩提本无树，明镜亦非台

佛家妙语

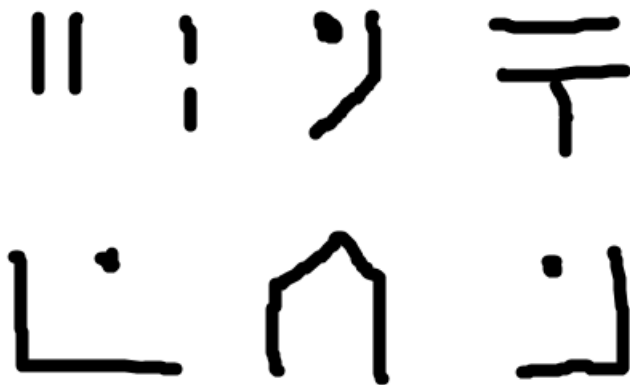
https://blog.csdn.net/weixin_44145820

第七关: 标准银河字母

//7. 剧情.txt

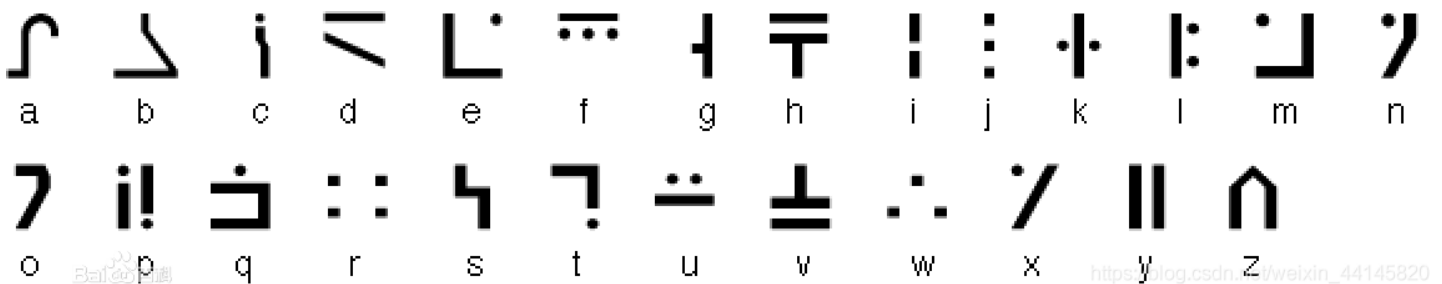
7. 进塔一看，4条腿的桌子上还有个啥台子？咋在往外冒字

7.png↓



https://blog.csdn.net/weixin_44145820

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

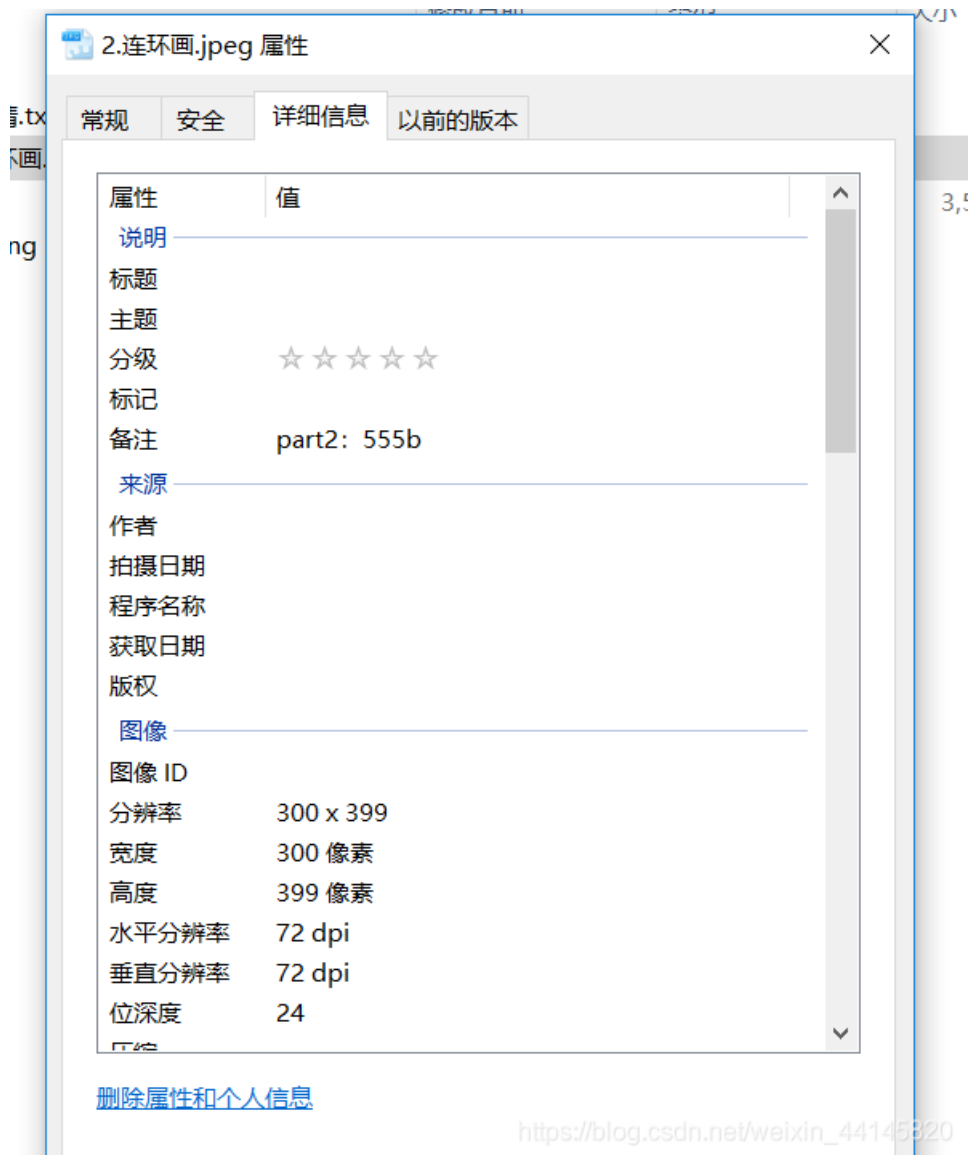
藏在1.连环画.png图片的末尾：part1:068c

1. 连环画.png		Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
1. 连环画.png	E:\CTF\misc\套娃\1	0005B2F0	7F	5C	77	79	76	C9	7C	F4	9B	D7	8A	0E	3B	50	7C	21	.\wyv? ?浞? ;P
文件大小:	365 KB 373,939 字节	0005B300	DA	3F	66	06	89	26	53	85	93	D6	DB	55	61	9B	2C	DE	? f.? S?搗跼a?,?
默认的编辑模式	原始	0005B310	BE	DB	1E	16	A4	1F	00	2A	E6	79	CE	AC	C0	A0	D6	59	聚..?*緇維罔諱
状态:	0	0005B320	0C	84	28	7A	D2	1F	F2	32	86	5F	46	03	06	4F	C6	E2	.?(z? ? 咩F..0柒
撤销级别:	n/a	0005B330	6F	F4	B5	FD	6E	BF	DB	7F	5C	E3	8E	56	6C	07	F1	B2	o?謀n?? \?嶸1.癩
撤销相反:	0	0005B340	B9	F6	17	7E	AA	FD	F5	1B	2D	09	18	CE	58	2D	DD	06	滾.~璫? -..?X-?
创建时间:	2020/02/14 17:34:31	0005B350	76	9E	1D	A9	78	4A	00	7C	BD	4B	8F	F2	E7	3F	B7	9D	v?.?xJ. 終.?? ?
最后写入时间:	2020/02/02 19:38:22	0005B360	D9	37	EB	BF	67	3D	CF	2C	DE	6D	40	1E	60	B2	FE	E0	? 脞g=? 辭@.`?
属性:	A	0005B370	E9	6B	00	C4	C8	E8	87	7F	16	7D	C9	F6	D8	5D	15	AB	閑.?辱?.)肾豸.?
图标:	0	0005B380	4A	5A	C6	86	0A	40	35	D0	8A	47	74	79	13	D5	58	E3	JZ茈.@5?隼ty.?X?
模式:	文本	0005B390	FA	EE	2B	77	59	C6	F7	A6	C7	9C	1A	5F	7A	28	3B	17	+wY?蠟蔗._z(;.
字符集:	ANSI ASCII	0005B3A0	DF	50	B9	C8	95	07	DE	4A	15	08	A3	C9	DC	C7	18	63	邊谷? 輻.. I 芮.c
偏移量:	16 进制	0005B3B0	0C	73	7B	B1	17	09	FF	EB	BF	FF	FD	FE	CD	94	1A	89	.s{?. ? 蛤.?
字节/页面:	36x16=576	0005B3C0	D1	DD	0C	C9	6E	D1	3D	6A	C7	51	41	88	E7	57	9E	1C	演.?n?=j苾A?縱?
窗口 #:	1	0005B3D0	75	1F	30	1E	6E	BE	5E	AA	61	EA	70	20	4D	49	CD	0B	u.0.n?^?a?p MI?
窗口编号:	1	0005B3E0	55	78	13	90	A1	A5	89	7F	66	50	71	6A	8B	B9	24	93	Ux.. ? fPqj嫻\$?
剪贴板:	可用	0005B3F0	27	67	A1	3F	09	F7	77	98	CB	8F	EF	AE	5F	BA	33	9F	'g? .?w?? 锂_?3?
临时文件夹:	12.1 GB 空闲	0005B400	A9	2F	37	23	A6	FB	01	EC	88	EB	DE	40	6B	1F	9D	5A	? ?# .?填轅k..Z
.Users\ASUS\AppData\Local\Temp		0005B410	CB	0E	7D	AB	23	C8	B0	7D	41	95	B2	BE	54	13	A3	C1	? }?#?體A?簿T.A
		0005B420	AC	14	64	1F	97	CB	E5	E5	5F	FF	FA	97	68	7A	75	9F	? d.梁邈_ 鷹hzu?
		0005B430	FE	6E	BF	DB	EF	76	B6	3B	F4	E5	57	AA	2F	7F	7D	2B	正扣脛? 翦w?/.)+
		0005B440	2E	AE	75	AC	E4	8B	B7	99	35	38	95	B4	F6	55	FF	3F	.?u?鏡窓58曠鯨 ?
		0005B450	D2	F6	A9	BB	F1	BF	AE	F3	88	89	74	6F	44	59	7C	C5	姻└奢鄴珍toDY ?
		0005B460	EB	B5	E5	85	DC	C2	10	FF	F5	5F	FF	F5	17	74	FD	77	氫錫房. 鮭 .t齣
		0005B470	FB	DD	7E	B7	DF	ED	77	FB	DD	7E	B7	DF	ED	AF	6A	BF	~?唔w?翱憤憑j?
		0005B480	A0	74	E4	EF	F6	BB	FD	6E	BF	DB	EF	F6	BB	FD	6E	BF	爐淖龔龔扣秭积n?
		0005B490	DB	DF	D9	FE	0F	A7	0E	85	27	60	EF	0F	5B	00	00	00	圻洗.?.?'`? [...
		0005B4A0	00	49	45	4E	44	AE	42	60	82	70	61	72	74	31	3A	30	.IEND?B`脩art1:0
		0005B4B0	36	38	63														68c

https://blog.csdn.net/weixin_44145320

2. 图片信息

右键打开2.连环画.png的属性，part2:555b

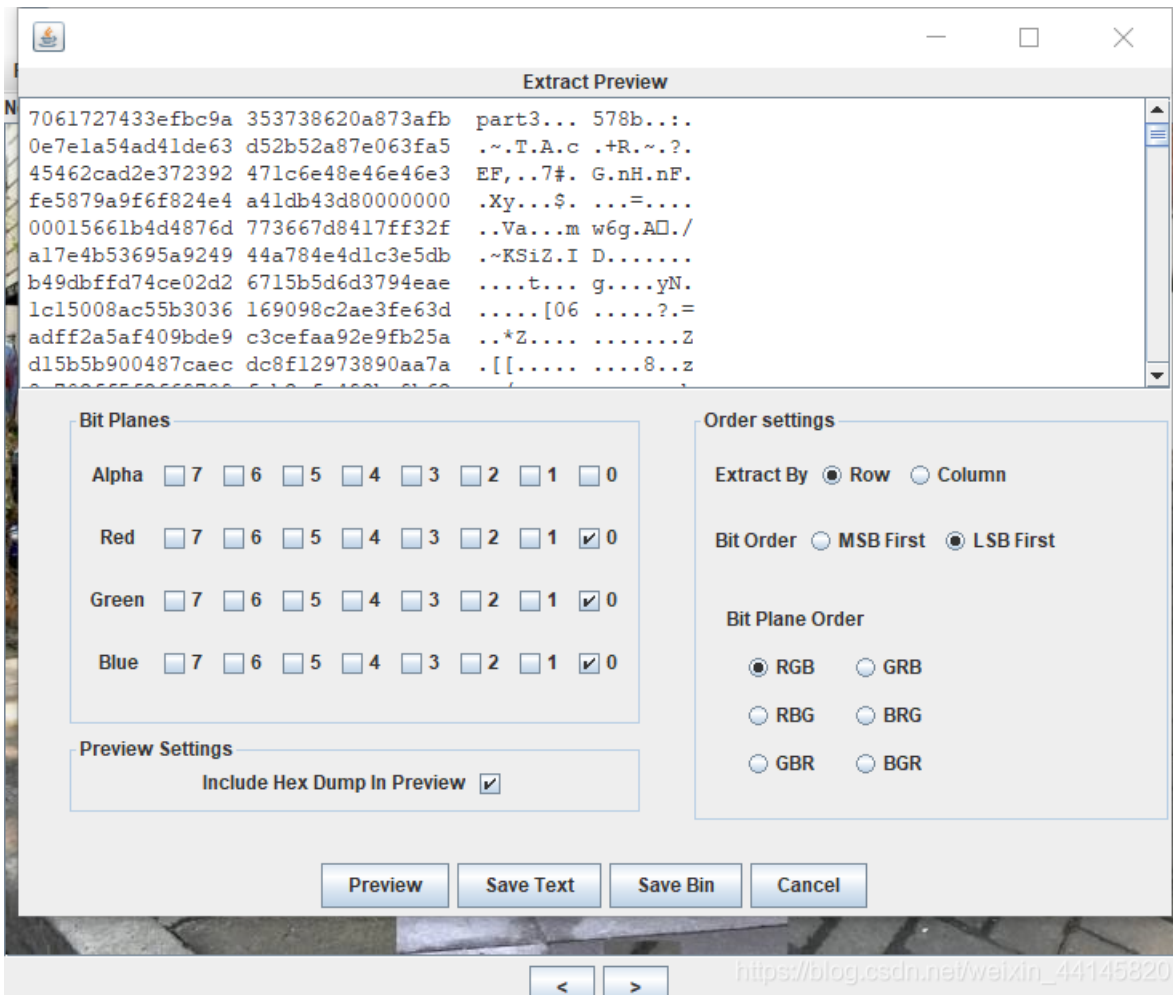


3.LSB隐写

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	擱NG..... IHDR
00000010	00	00	04	38	00	00	09	06	08	06	00	00	00	39	8E	1A	...8...? ?
00000020	D4	00	00	00	01	73	52	47	42	00	AE	CE	1C	E9	00	00	? ...sRGB. 横. ?..
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...?...?..?

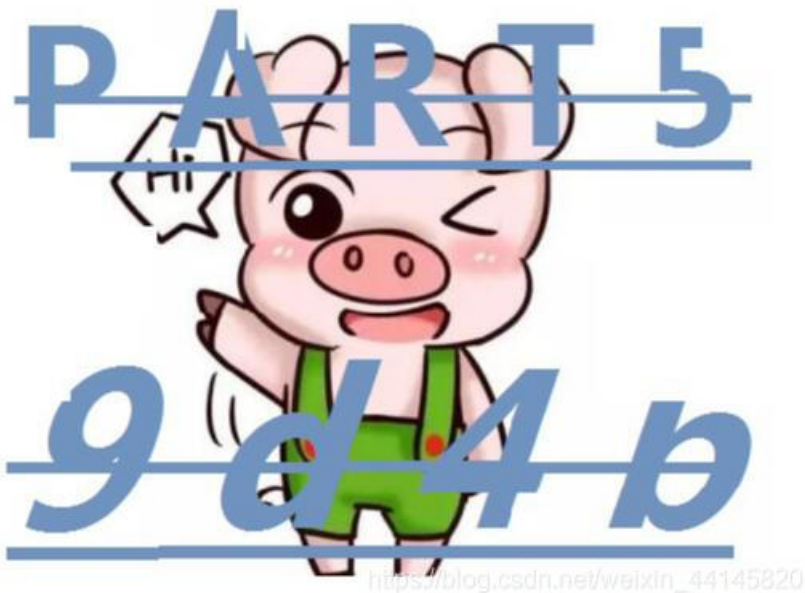


这里还有一个小技巧，如果图片高度被修改过，Kali Linux是打不开的

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
```



```
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

```
10202020101010101020201010101020102020201010201010202020102010101010202010202020101020202010102020201020101010202010202020102010101020202010102020201020101010202020102010101020201020101010202010201010102020102010102010102010102010
```

然后把10转化为0,20转为1，脚本如下

```
s = "1020202010101010102020101010102010202020101020101020202010201010101020201020202010201010102020102020201020101010202010202020102010101020201020101010202010201010102020102010102010102010"
s = s.replace("10", "0")
s = s.replace('20', '1')
print s
```

得到01串: 0111000001100001011100100111010000110111001110100011011000110001001101010011011000110010

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??

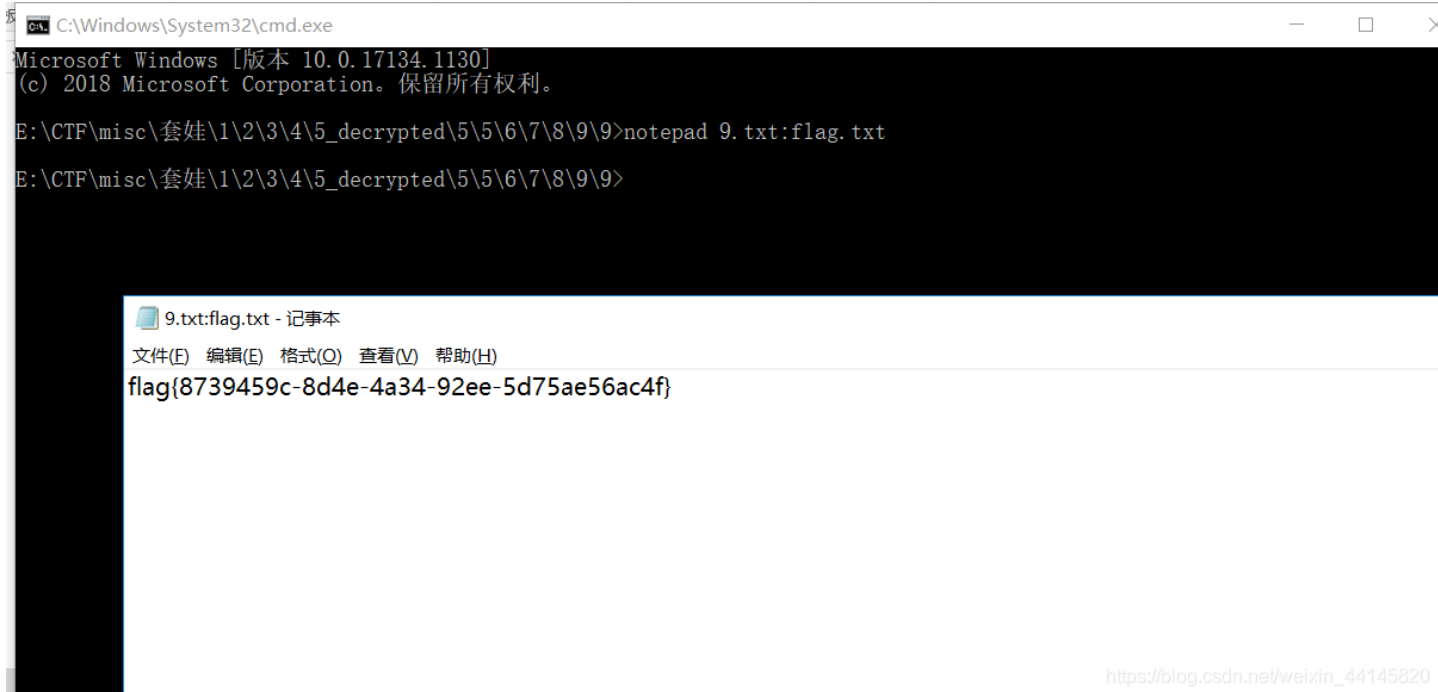
使用lads.exe查看一下:

```
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](#)
