2018山东省科来杯writeup

原创

菜鸟头头 于 2018-11-06 19:44:18 发布 922 收藏
分类专栏： write up

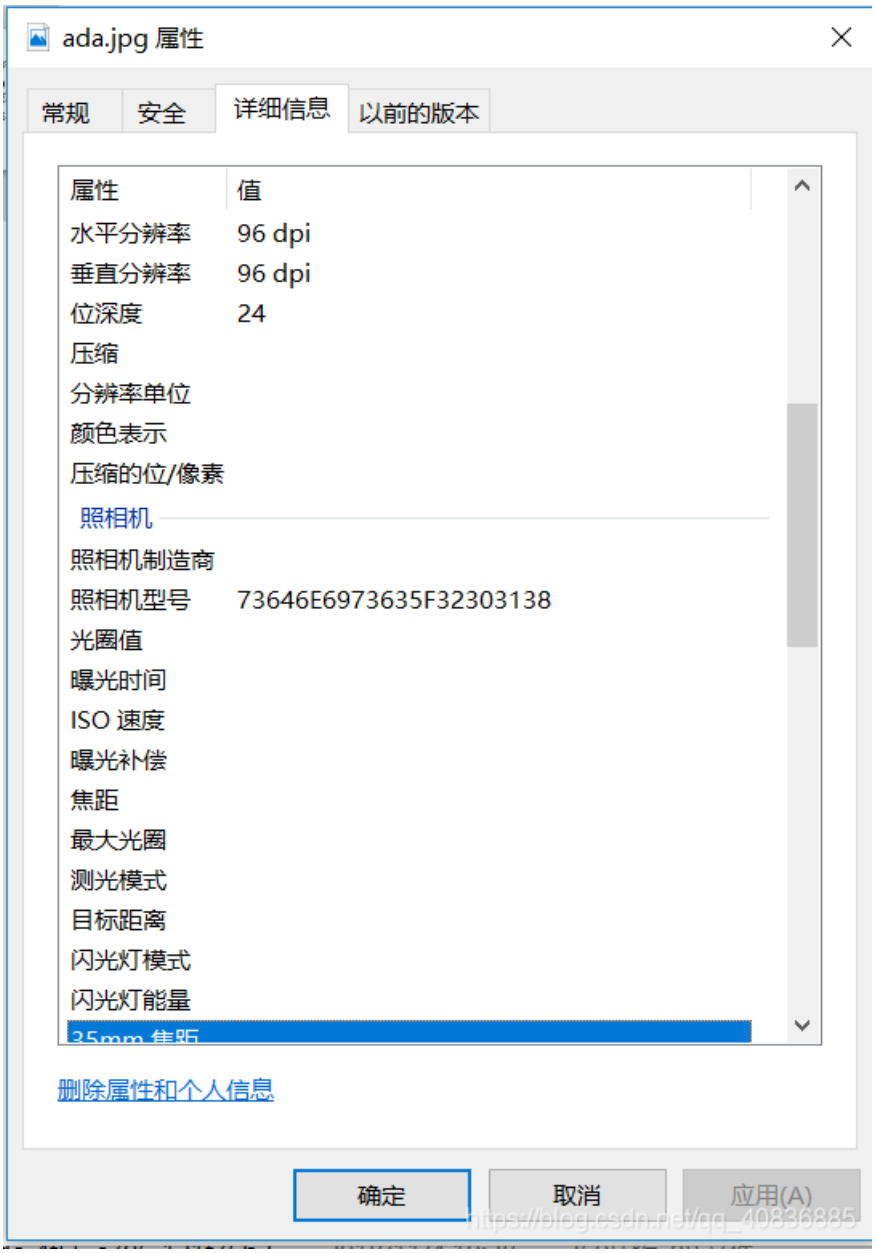

write up 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

1.呵哒

2018科来杯writeup

1.呵哒：

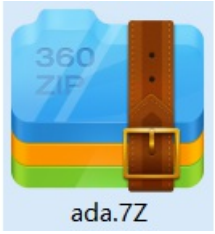
查看图片属性，得到照相机型号那一栏



仔细分析得：为十六进制的一个密码：分析可能是一个压缩包

然后更改图片后缀名。

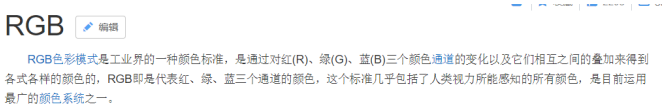
ZIP 、RAR、 7Z发现RAR和7Z能用



用刚才十六进制解得密码输入就得到：flag{3XiF_iNf0rM@ti0n}

2.basic

打开一看是RGB，所以想着这个可能是要把255 255 255转变成为图片来解题

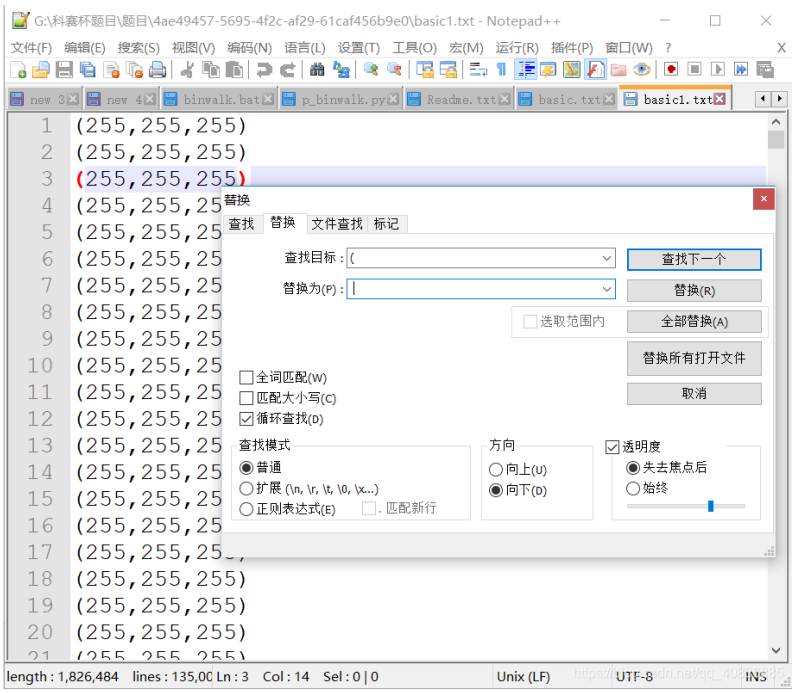


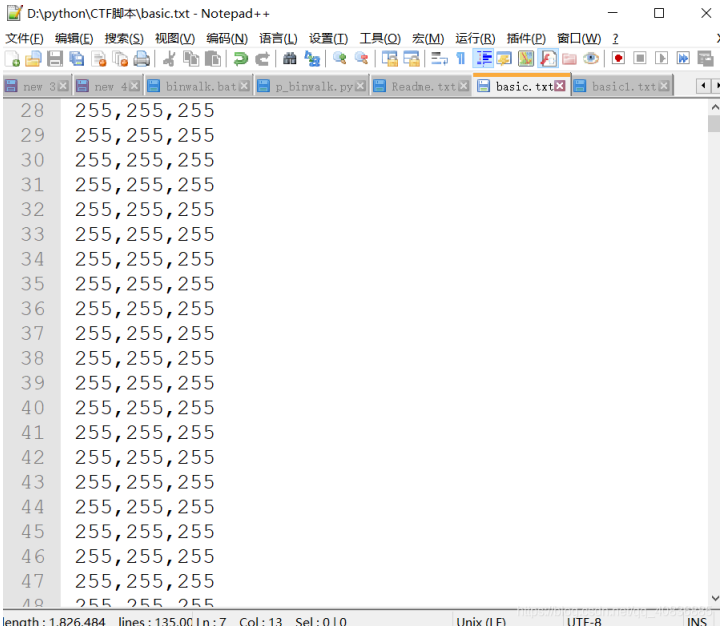
所以到这里去网上找了个大佬的代码

```
#像素转化为图片
from PIL import Image
import re
x = 50 #x坐标  通过对txt里的行数进行整数分解
y = 2700 #y坐标  x*y = 行数
im = Image.new("RGB",(x,y))#创建图片
file = open('basic.txt') #打开rbg值文件

#通过一个个rgb点生成图片
for i in range(0,x):
    for j in range(0,y):
        line = file.readline()#获取一行
        rgb = line.split(",")#分离rgb
        im.putpixel((i,j),(int(rgb[0]),int(rgb[1]),int(rgb[2])))#rgb转化为像素
im.show()
```

使用代码的使用需要将txt中（255,255,255）的括号去掉改成255,255,255，在这里我使用的notepad++来修改，Ctrl+H打开替换功能：将()都去掉





改成这样，在将文件放入python代码里面运行。

得到这个图片，这个就靠眼力了！

得到flag{RGB_1s_e4sY}

3.

y = 17*x-8 flag{szzyfimhyzd}

这个是

仿射密码：加密算法：c = a*m + b(mod n)大概就是这么回事儿，我也没有仔细研究！

其中a=17，b=-8 ，n=szzyfimhyzd，然后使用工具解得

这样就可以得到flag{affineshift}

4.二进制、八进制、十进制、十六进制，你能分的清吗？

```
d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101
b1101100 o141 d105 x62 d101 b1101001 d46 o40 d71 x69 d118 x65 x20 b1111001
o157 b1110101 d32 o141 d32 d102 o154 x61 x67 b100000 o141 d115 b100000
b1100001 d32 x67 o151 x66 d116 b101110 b100000 d32 d102 d108 d97 o147 d123
x31 b1100101 b110100 d98 d102 b111000 d49 b1100001 d54 b110011 x39 o64
o144 o145 d53 x61 b1100010 b1100011 o60 d48 o65 b1100001 x63 b110110 d101
o63 b111001 d97 d51 o70 d55 b1100010 d125 x20 b101110 x20 b1001000 d97
d118 o145 x20 d97 o40 d103 d111 d111 x64 d32 o164 b1101001 x6d o145 x7e
```

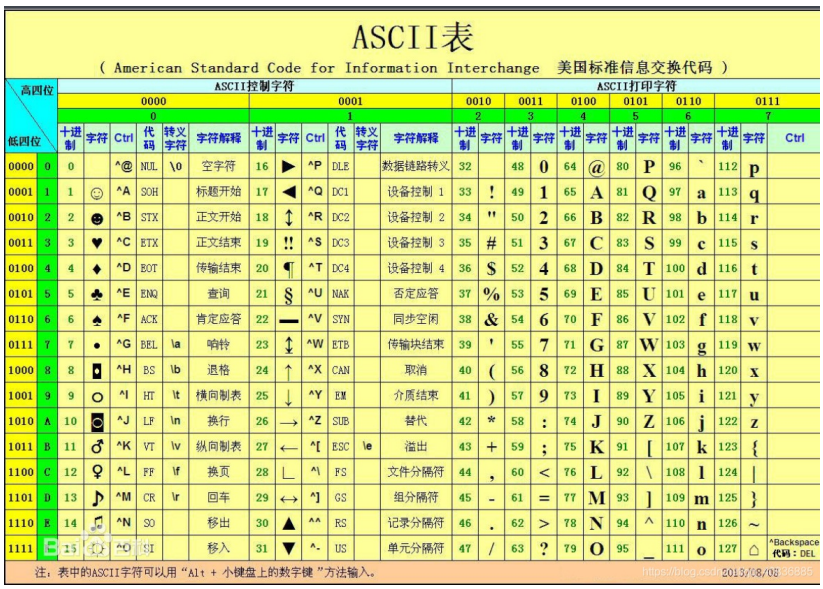
这里面x（hexadecimal）表示十六进制、o（Octor）表示八进制、D(Decimal)表示的十进制、b（binary）表示二进制。

我比较菜大佬们都是用代码区分在直接的flag{}，而我当时做的时候是一个一个的换的，感觉比较low和浪费时间，所以去网上把

大佬的代码copy了下来，自己去理解了一遍;在这里附上大佬代码

```
import binascii
text = "d87 x65 x6c x63 o157 d109 o145 b100000 d116 b1101111 o40 x6b b1100101 b1101100 o141 d105 x62 d101 b
solution = ''
text2 = text.split(' ')
for x in text2:
    print(x)
    if x[0] == 'b': #binary
        solution += chr(int(x[1:],2))
    elif x[0] == 'x': # hexadecimal
        solution += chr(int(x[1:],16))
    elif x[0] == 'd': # decimal
        solution += chr(int(x[1:]))
    elif x[0] == 'o': # octal
        solution += chr(int(x[1:],8))
print(solution)
```

随便附上一张ASCII表（不会写脚本一个一个转换好，对照，哈哈哈！）



ASCII表

(American Standard Code for Information Interchange 美国标准信息交换代码)

高四位 / 低四位	0000						0001						0010		0011		0100		0101		0110		0111		
	ASCII控制字符												ASCII打印字符												
	0						1						2		3		4		5		6		7		
	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0		^@	NUL	\0	空字符	16	▶	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	☺	^A	SOH		标题开始	17	◀	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂

*Backspace 代码：DEL

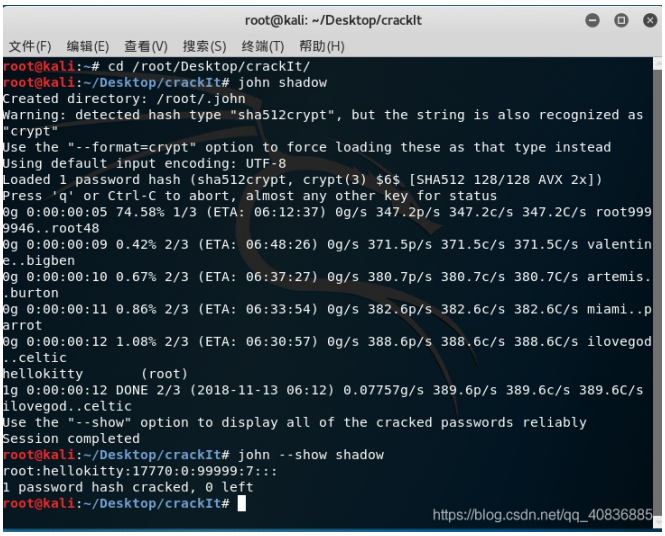
注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。

2013/08/08

5.shadow

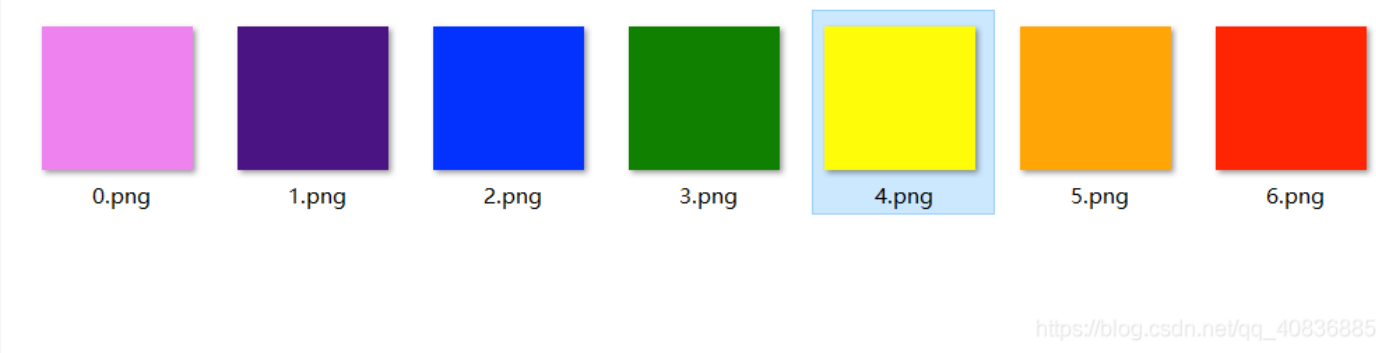
进入shadow文件夹，

执行John shadow命令，等他自己跑 然后就可以得到flag{hellokitty}

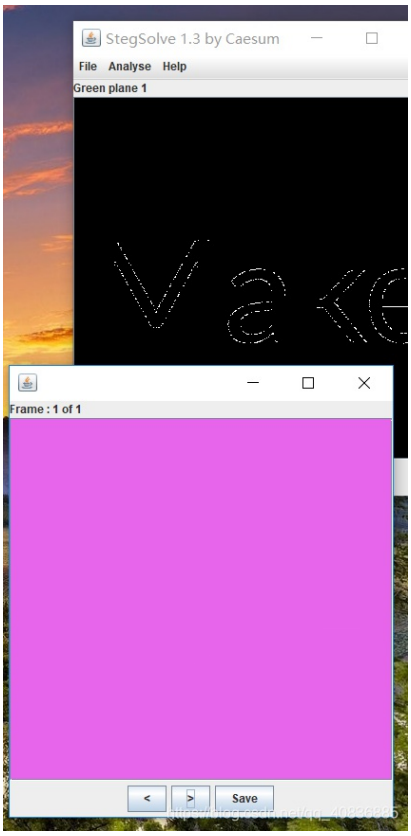


6.你见过彩虹吗？

通过解压文件看到里面是七张图片

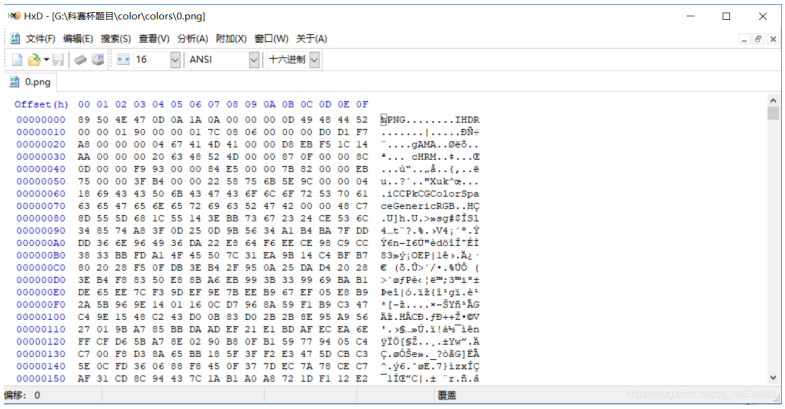


先用stegslove这个软件跑一下



看了下这些，感觉好像没什么有用的，所以在这里我们想到该下图片的长度，看看是不是

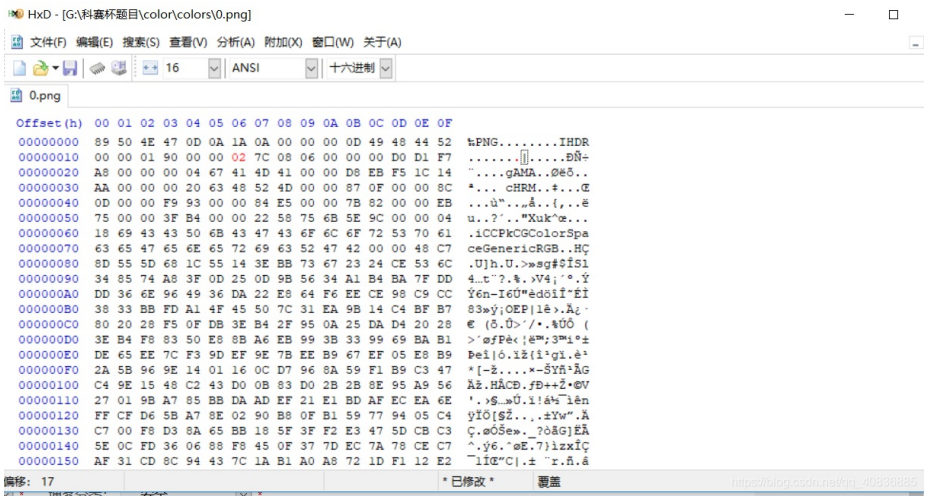
有什么，用HxD来改下



这个第二行的前四位是图片的宽度

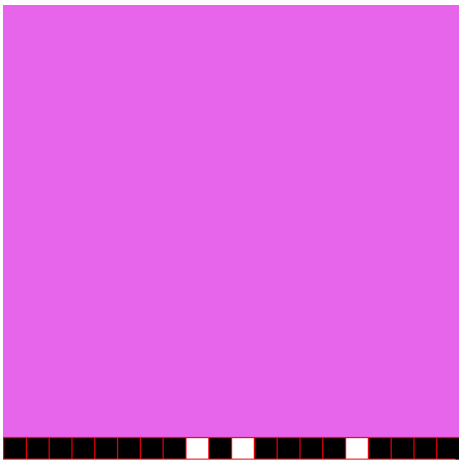
后四位是图片的高度

在这里我们修改高度看看，将第二行的高度第三个数据由01改成02



在保存设置得到不一样的图片，看到下面有黑白两种空格，所以猜想是二进制，七张图片各有一个二进制编码

在这里我就写一个示范



所以就用python编写了脚本，当然代码时看着大佬的代码自己理解一下敲得

```
#coding:utf-8
c1 = '11111111010111101111';
c2 = '11111011111110111111';
c3 = '00001100101010110001';
c4 = '01001010010000001101';
c5 = '11010011011101010111';
c6 = '10011011011010110110';
c7 = '00111001101101111101';
flag = ''
for i in range(0,20):#遍历c1...c7
    c = c1[i]+c2[i]+c3[i]+c4[i]+c5[i]+c6[i]+c7[i]
    flag +=chr(int(c,2))#将二进制转化为ASCII
print(flag)
```

然后就得到

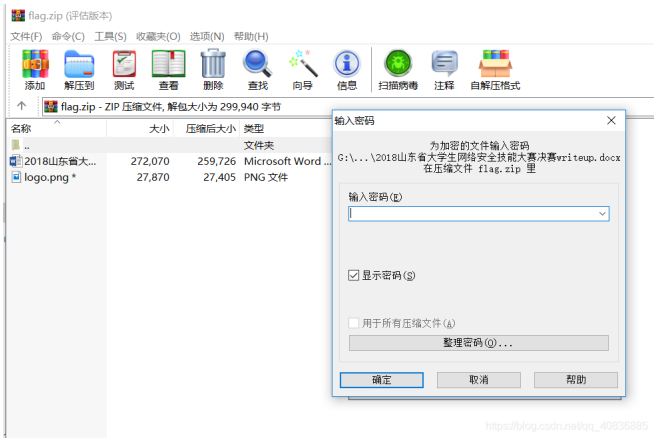
flag{Png1n7erEs7iof}

7.神秘的文件

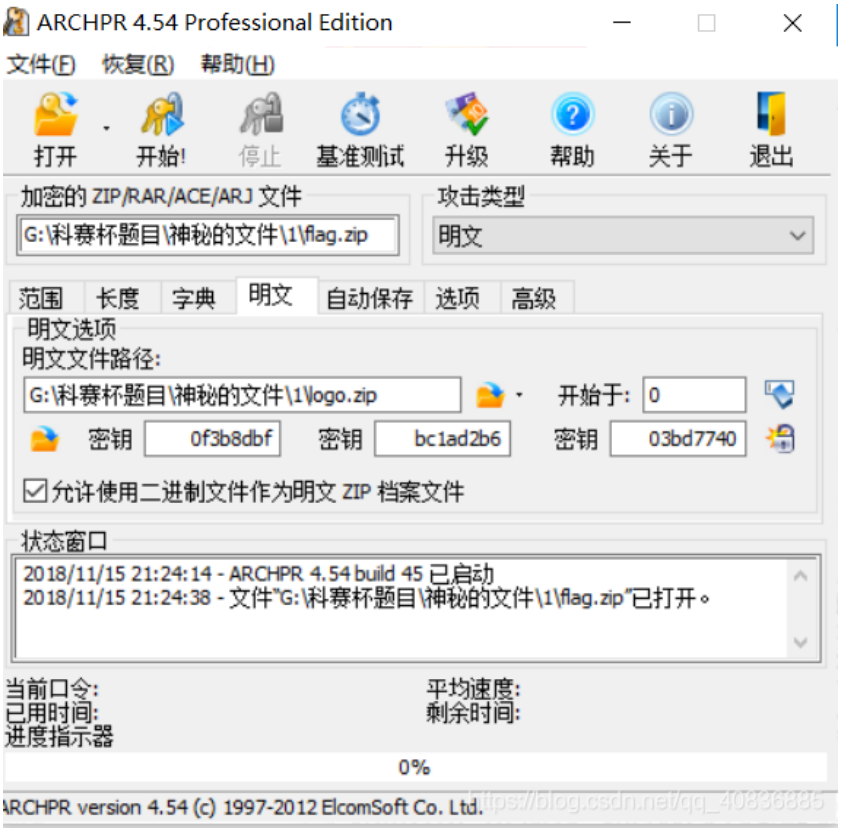
先解压，得到：

在解压flag.zip,但是发现要密码，但我们发现压缩包里面有一个和外面图片一样名字的图片，所以猜想是明文碰撞，

所以用WinRAR将外面的logo.png图片压缩为一个压缩包



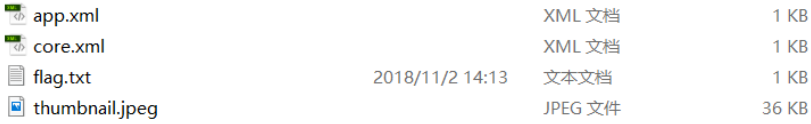
这里我们要用到一款暴力破解软件ARCHPR，进行明文破解



两个压缩文件的位置一定要放对，上面放flag.zip 下面的放logo.zip

完成后我们会获得这个文件的口令，这个口令就是flag.zip的密码，解压后会得到一个Word文档

里面是一个滑稽脸，我们再把文档的后缀名改成zip，在进行解压，然后逐个寻找



你会找到一个flag.txt

进去，得到flag，但是里面是base64的编码，再用软件一解

```
ZmxhZ3tkMGNYXzFzX3ppUF9maWxlfQ==
```

```
结果：(字符数统计：22)
flag{d0cX_1s_ziP_file}
```


得到：flag{d0cX_1s_ziP_file}