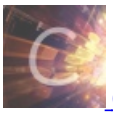
BUUCTF Misc杂项前十二道题的思路和感悟

原创

别害怕我在 于 2021-08-18 17:45:48 发布 995 收藏 28

分类专栏： CTF杂项MISC新手 文章标签： CTF Misc writeup BUUCTF



---

title: BUUCTF Misc
date: 2021年8月18日 17点27分
tags: MISC
categories: MISC

1、BUUCTF 签到题

直接告诉了flag。

2、BUUCTF 第二道题(Stegsolve)

下载附件之后，得到一个gif动图。

使用Stegsolve打开。

使用gif动图工具，

然后一张一张的向后翻，

得到flag{he11ohongke}

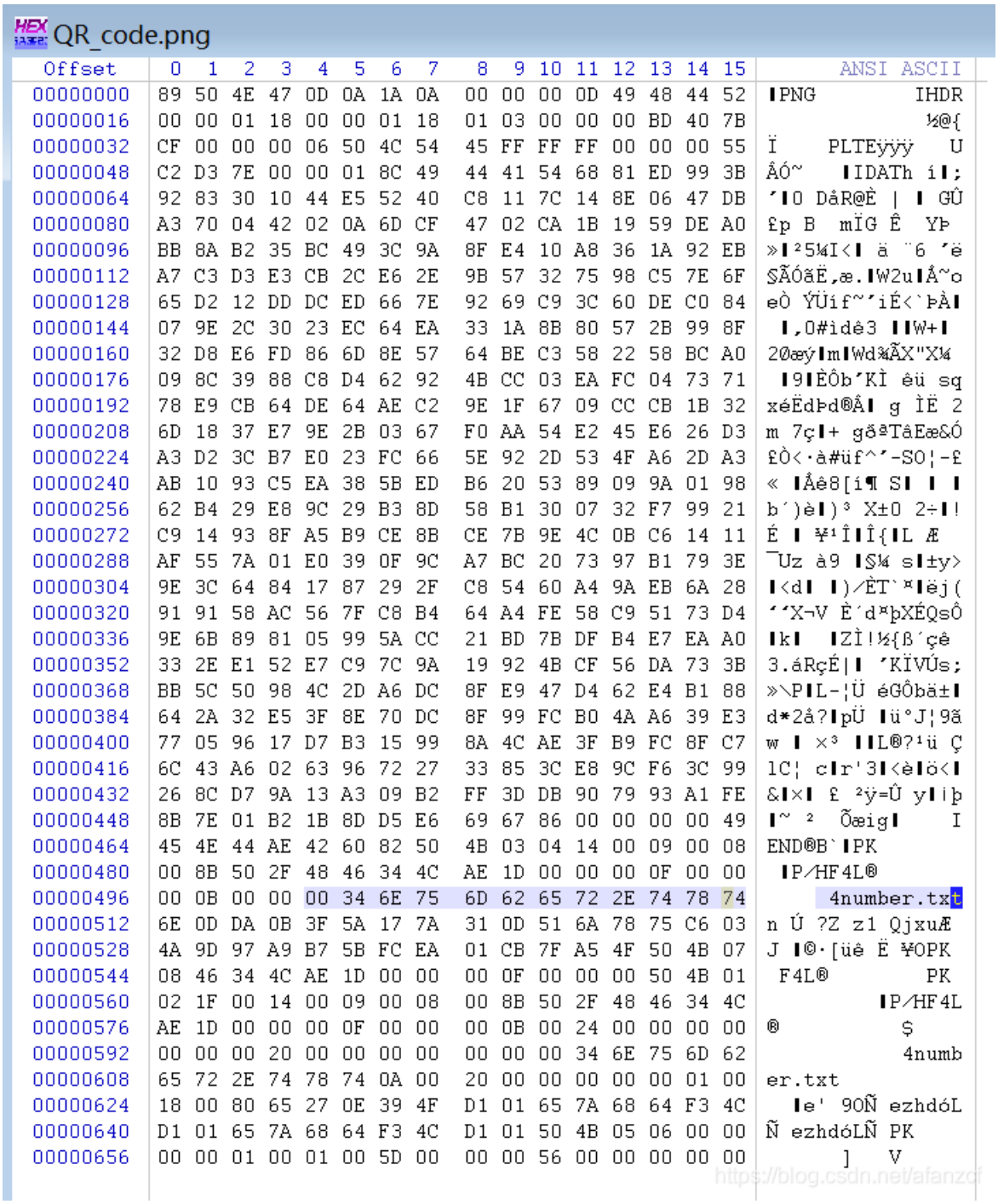
3、BUUCTF 二维码（QR Research、Ziperrllo、winhex）

下载附件之后是一个zip压缩包。

解压之后得到了一个png的二维码图片。

利用QR Research工具，扫描得到了一个不是flag的信息。

发现问题并不简单，根据之前攻防世界misc几道题的经验，应该是有东西藏在图片里面，直接拖到winhex打开。



QR_code.png

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	‰PNG IHDR
00000016	00	00	01	18	00	00	01	18	01	03	00	00	00	BD	40	7B	½@{
00000032	CF	00	00	00	06	50	4C	54	45	FF	FF	FF	00	00	00	55	Ï PLTEÿÿÿ U
00000048	C2	D3	7E	00	00	01	8C	49	44	41	54	68	81	ED	99	3B	ÂÓ~ IDATh í;
00000064	92	83	30	10	44	E5	52	40	C8	11	7C	14	8E	06	47	DB	’0 DåR@È | G Û
00000080	A3	70	04	42	02	0A	6D	CF	47	02	CA	1B	19	59	DE	A0	£p B mÏG Ê YÞ
00000096	BB	8A	B2	35	BC	49	3C	9A	8F	E4	10	A8	36	1A	92	EB	»²5¼I< ä ¨6 ’ë
00000112	A7	C3	D3	E3	CB	2C	E6	2E	9B	57	32	75	98	C5	7E	6F	§ÃÓãË,æ.W2uÅ~o
00000128	65	D2	12	DD	DC	ED	66	7E	92	69	C9	3C	60	DE	C0	84	eÒ ÝÜíf~’iÉ<`ÞÀ
00000144	07	9E	2C	30	23	EC	64	EA	33	1A	8B	80	57	2B	99	8F	,0#ìdê3 W+
00000160	32	D8	E6	FD	86	6D	8E	57	64	BE	C3	58	22	58	BC	A0	2Øæý m Wd¾ÃX"X¼
00000176	09	8C	39	88	C8	D4	62	92	4B	CC	03	EA	FC	04	73	71	9 ÈÔb’KÌ êü sq
00000192	78	E9	CB	64	DE	64	AE	C2	9E	1F	67	09	CC	CB	1B	32	xéËdÞd®Â g ÌË 2
00000208	6D	18	37	E7	9E	2B	03	67	F0	AA	54	E2	45	E6	26	D3	m 7ç+ gðªTâEæ&Ó
00000224	A3	D2	3C	B7	E0	23	FC	66	5E	92	2D	53	4F	A6	2D	A3	£Ò<·à#üf^’-SO¦-£
00000240	AB	10	93	C5	EA	38	5B	ED	B6	20	53	89	09	9A	01	98	« Åê8[í¶ S š
00000256	62	B4	29	E8	9C	29	B3	8D	58	B1	30	07	32	F7	99	21	b´)è)³ X±0 2÷!
00000272	C9	14	93	8F	A5	B9	CE	8B	CE	7B	9E	4C	0B	C6	14	11	É ¥¹Î Î{ L Æ
00000288	AF	55	7A	01	E0	39	0F	9C	A7	BC	20	73	97	B1	79	3E	¯Uz à9 §¼ s±y>
00000304	9E	3C	64	84	17	87	29	2F	C8	54	60	A4	9A	EB	6A	28	<d)/ÈT`¤ëj(
00000320	91	91	58	AC	56	7F	C8	B4	64	A4	FE	58	C9	51	73	D4	’’X¬V È´d¤þXÉQsÔ
00000336	9E	6B	89	81	05	99	5A	CC	21	BD	7B	DF	B4	E7	EA	A0	k ZÌ!½{ß´çê
00000352	33	2E	E1	52	E7	C9	7C	9A	19	92	4B	CF	56	DA	73	3B	3.áRçÉ| ’KÏVÚs;
00000368	BB	5C	50	98	4C	2D	A6	DC	8F	E9	47	D4	62	E4	B1	88	»\P L-¦Ü éGÔbä±
00000384	64	2A	32	E5	3F	8E	70	DC	8F	99	FC	B0	4A	A6	39	E3	d*2å? pÜ üºJ¦9ã
00000400	77	05	96	17	D7	B3	15	99	8A	4C	AE	3F	B9	FC	8F	C7	w × ³ L®?¹ü Ç
00000416	6C	43	A6	02	63	96	72	27	33	85	3C	E8	9C	F6	3C	99	lC¦ c r'3 <è ö<
00000432	26	8C	D7	9A	13	A3	09	B2	FF	3D	DB	90	79	93	A1	FE	& ×£ ²ÿ=Û y¡þ
00000448	8B	7E	01	B2	1B	8D	D5	E6	69	67	86	00	00	00	00	49	~ ² ÕæigI
00000464	45	4E	44	AE	42	60	82	50	4B	03	04	14	00	09	00	08	END®B`PK
00000480	00	8B	50	2F	48	46	34	4C	AE	1D	00	00	00	0F	00	00	P/HF4L®
00000496	00	0B	00	00	00	34	6E	75	6D	62	65	72	2E	74	78	74	4number.txt
00000512	6E	0D	DA	0B	3F	5A	17	7A	31	0D	51	6A	78	75	C6	03	n Ú ?Z z1 QjxuÆ
00000528	4A	9D	97	A9	B7	5B	FC	EA	01	CB	7F	A5	4F	50	4B	07	J ©·[üê Ë ¥OPK
00000544	08	46	34	4C	AE	1D	00	00	00	0F	00	00	00	50	4B	01	F4L® PK
00000560	02	1F	00	14	00	09	00	08	00	8B	50	2F	48	46	34	4C	P/HF4L
00000576	AE	1D	00	00	00	0F	00	00	00	0B	00	24	00	00	00	00	® $
00000592	00	00	00	20	00	00	00	00	00	00	00	34	6E	75	6D	62	4numb
00000608	65	72	2E	74	78	74	0A	00	20	00	00	00	00	00	01	00	er.txt
00000624	18	00	80	65	27	0E	39	4F	D1	01	65	7A	68	64	F3	4C	e' 9OÑ ezhdóL
00000640	D1	01	65	7A	68	64	F3	4C	D1	01	50	4B	05	06	00	00	Ñ ezhdóLÑ PK
00000656	00	00	01	00	01	00	5D	00	00	00	56	00	00	00	00	00	] V

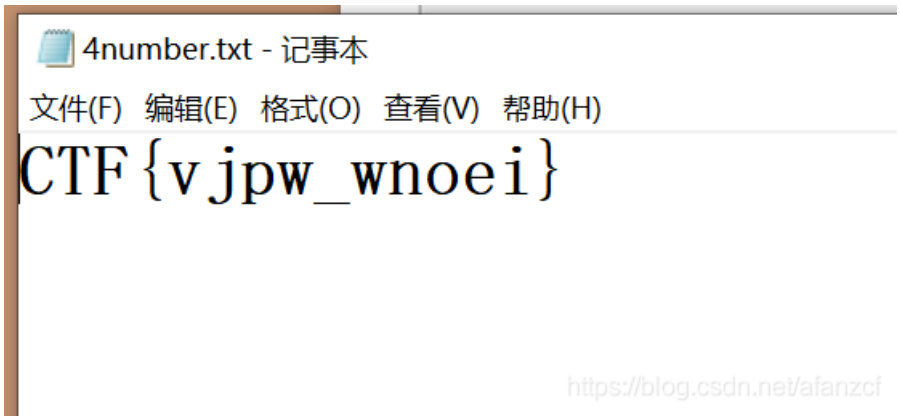
发现里面有一个txt文件。

猜想应该是涉及到了分离工具foremost。

但是电脑没装kali，于是把后缀改为zip试试。

居然打开了，但是可以看到这个txt需要密码，根据它文件名的提示，我们知道这是一个4位数的密码，于是用Ziperrllo暴力破解密码。

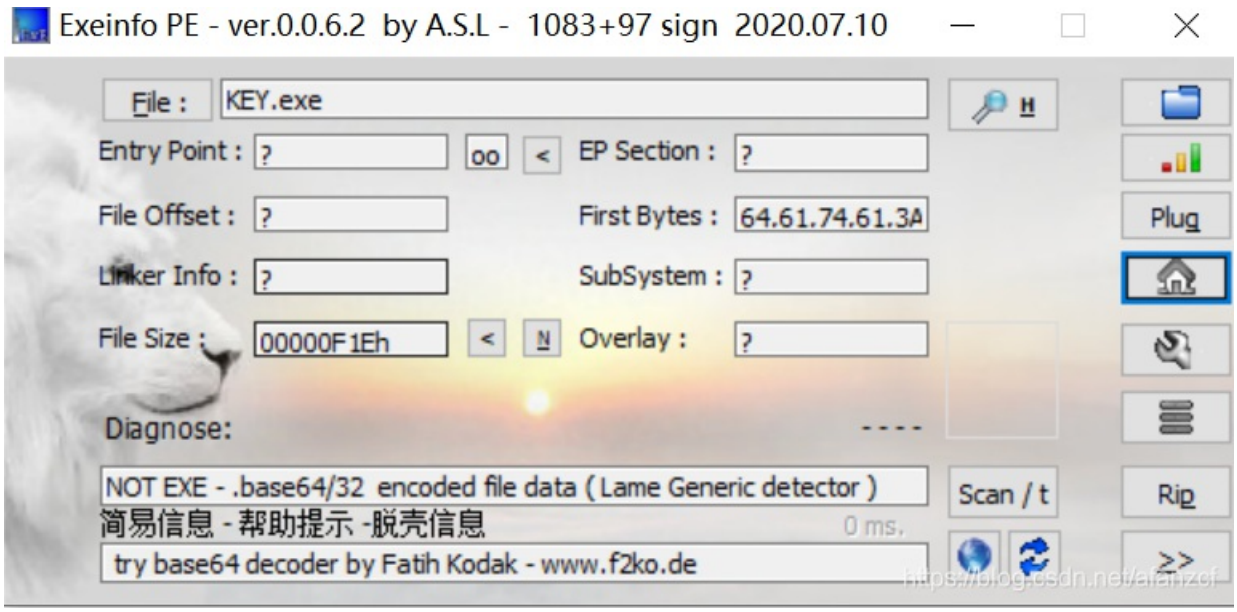
得到密码7639，然后打开txt，得到flag。



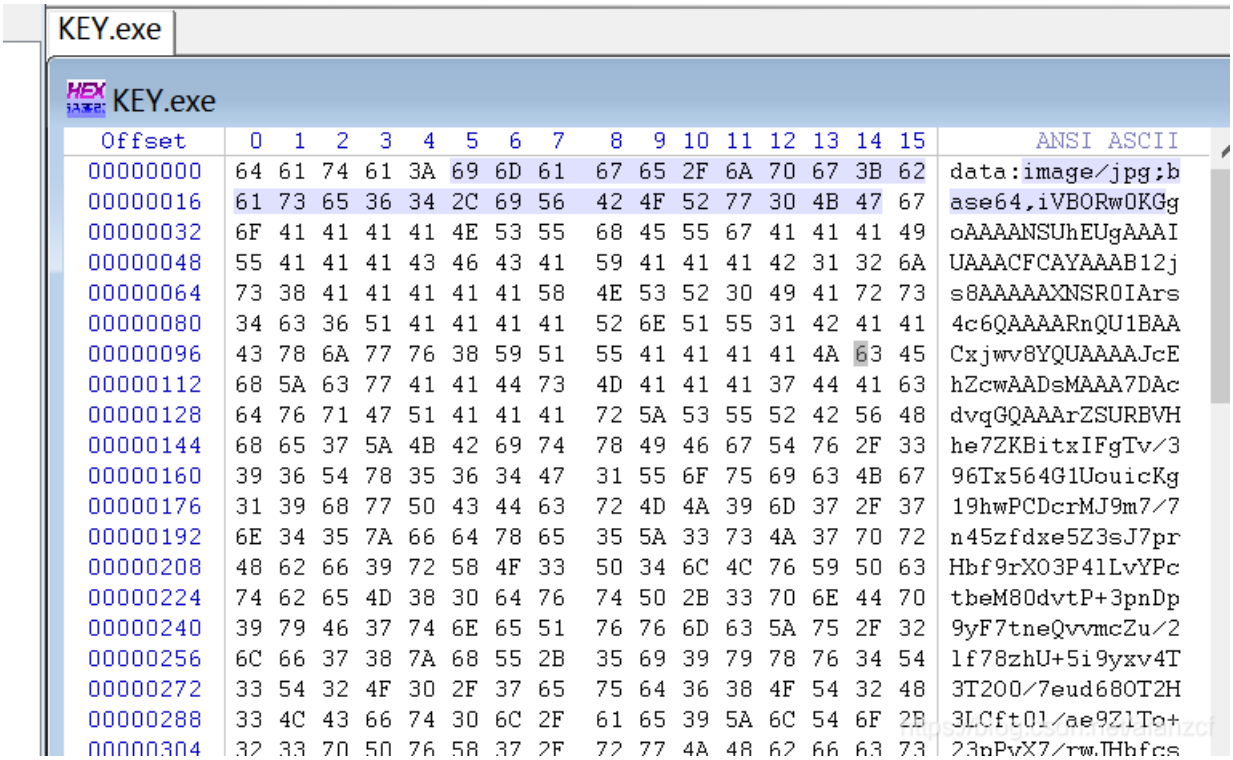
flag{vjpw_wnoei}

4、BUUCTF N种方法解决（base64转图片、直接网址打开）

下载题目附件之后，得到了一个exe文件，准备打开这个exe，却发现打不开。用PE查一下。



发现并不是exe文件，用winhex打开。



发现并不简单，类似于base64，但是又有图片。想到了base64转图片。

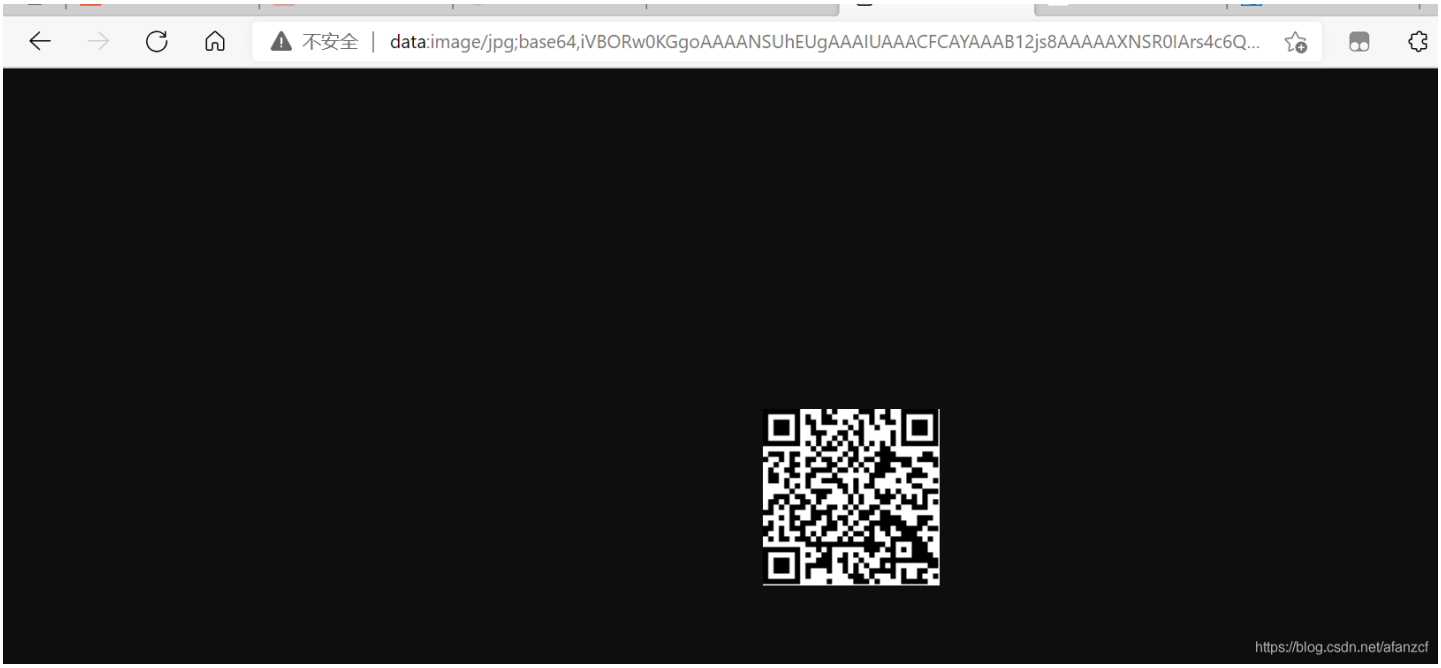
用notepad打开文件。

```

```

全选复制。

（1）直接拉到网站打开



扫描二维码，得到flag。

（2）在线base64转图片

base64图片在线转换工具 - 站长工具 (chinaz.com)

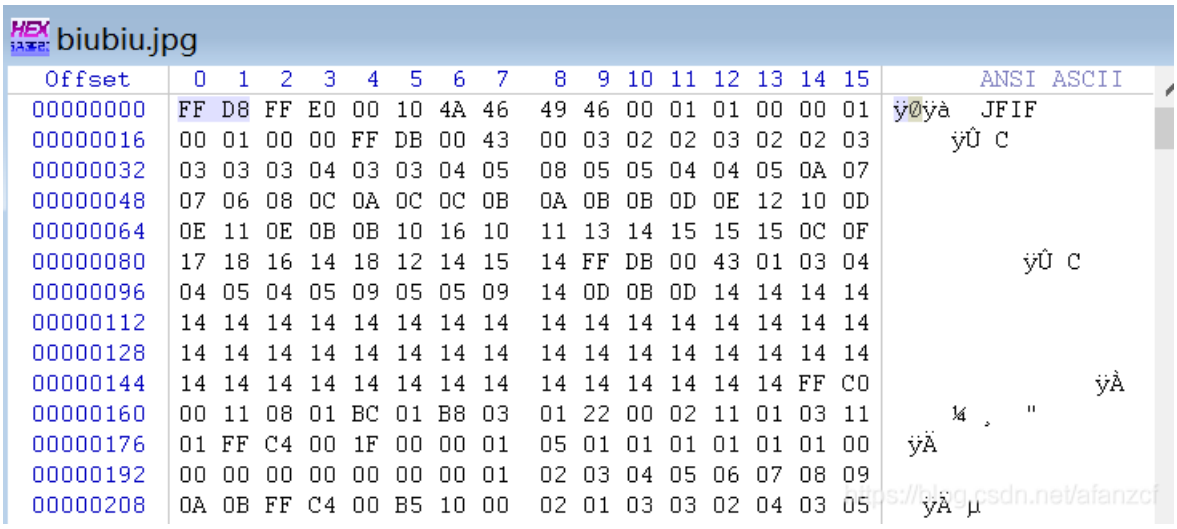
扫描二维码，得到flag

KEY{dca57f966e4e4e31fd5b15417da63269}

5、你竟然赶我走（winhex、Stegsolve）

（1）自己靠运气解出（解法一winhex）

下载附件之后，一个压缩包，解压之后，打开一张图片，并没有什么消息。用winhex打开。


biubiu.jpg

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿà JFIF
00000016	00	01	00	00	FF	DB	00	43	00	03	02	02	03	02	02	03	ÿÛ C
00000032	03	03	03	04	03	03	04	05	08	05	05	04	04	05	0A	07	
00000048	07	06	08	0C	0A	0C	0C	0B	0A	0B	0B	0D	0E	12	10	0D	
00000064	0E	11	0E	0B	0B	10	16	10	11	13	14	15	15	15	0C	0F	
00000080	17	18	16	14	18	12	14	15	14	FF	DB	00	43	01	03	04	ÿÛ C
00000096	04	05	04	05	09	05	05	09	14	0D	0B	0D	14	14	14	14	
00000112	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	
00000128	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	
00000144	14	14	14	14	14	14	14	14	14	14	14	14	14	14	FF	C0	ÿÀ
00000160	00	11	08	01	BC	01	B8	03	01	22	00	02	11	01	03	11	¼ ¸ "
00000176	01	FF	C4	00	1F	00	00	01	05	01	01	01	01	01	01	00	ÿÄ
00000192	00	00	00	00	00	00	00	01	02	03	04	05	06	07	08	09	
00000208	0A	0B	FF	C4	00	B5	10	00	02	01	03	03	02	04	03	05	ÿÄ µ

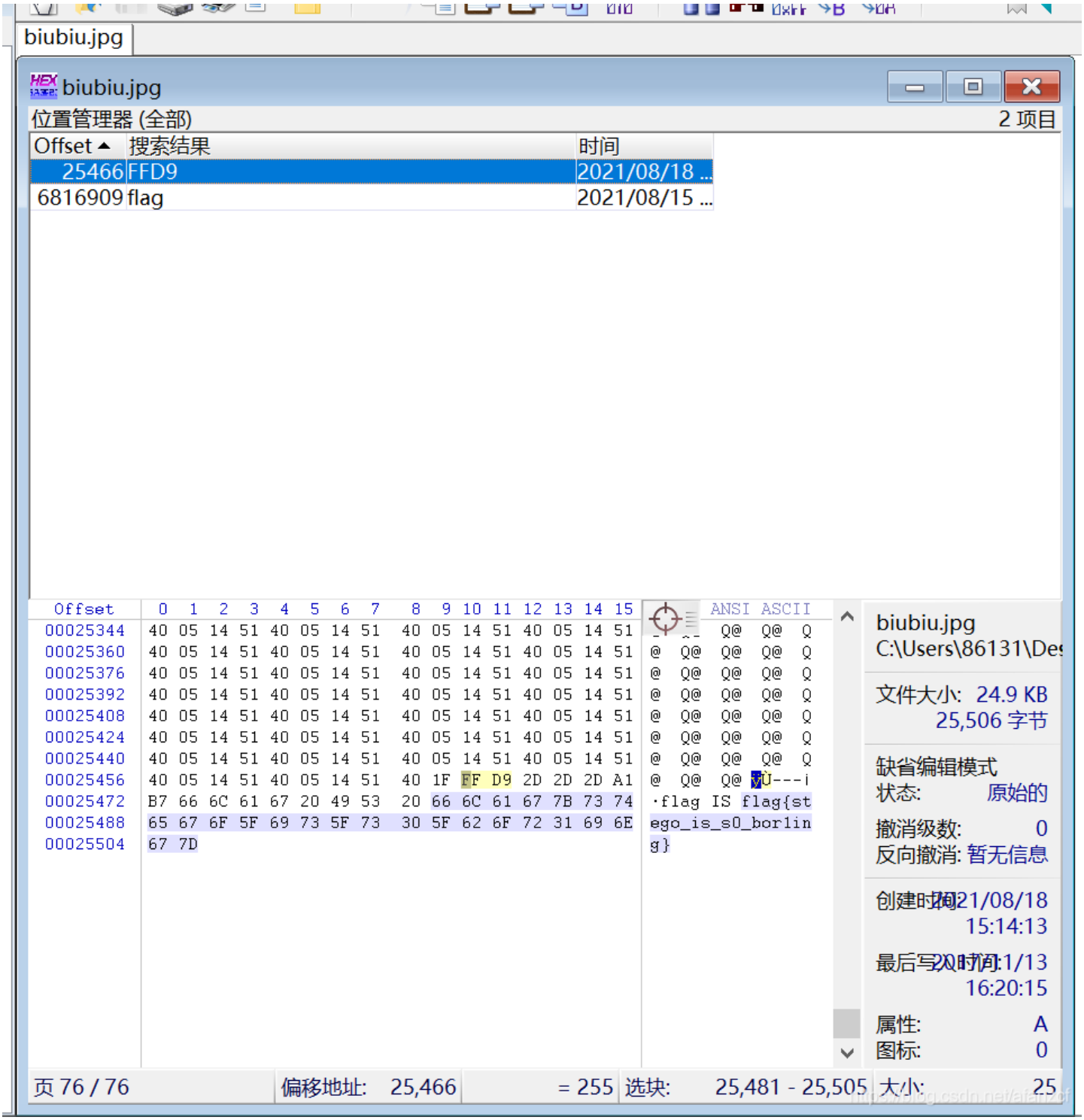
看到一个FFD8，jpg的一个文件头，我本来想找一下jpg的文件尾，FFD9的，就直接拉到最后。

00025312	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025328	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025344	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025360	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025376	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025392	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025408	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025424	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025440	40	05	14	51	40	05	14	51	40	05	14	51	40	05	14	51	@ Q@ Q@ Q@ Q
00025456	40	05	14	51	40	05	14	51	40	1F	FF	D9	2D	2D	2D	A1	@ Q@ Q@ ÿÙ---¡
00025472	B7	66	6C	61	67	20	49	53	20	66	6C	61	67	7B	73	74	·flag IS flag{st
00025488	65	67	6F	5F	69	73	5F	73	30	5F	62	6F	72	31	69	6E	ego_is_s0_bor1in
00025504	67	7D															g}

发现了flag？复制到，BUUCTF，对了。。。

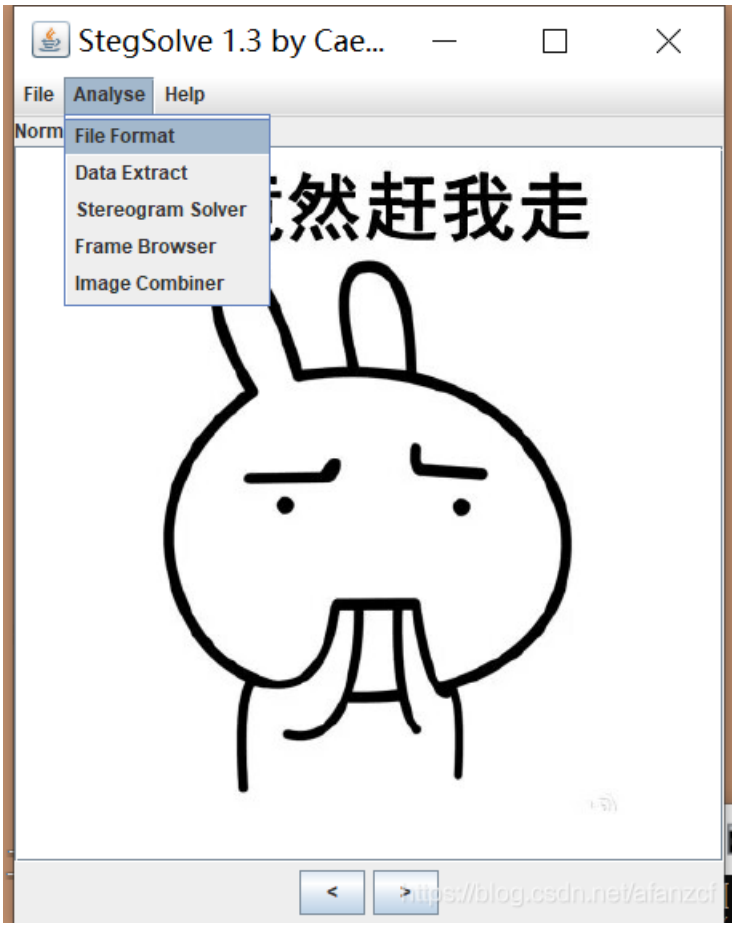
flag{stego_is_s0_bor1ing}

这里直接winhex里面十六进制搜索FFD9，也能出来

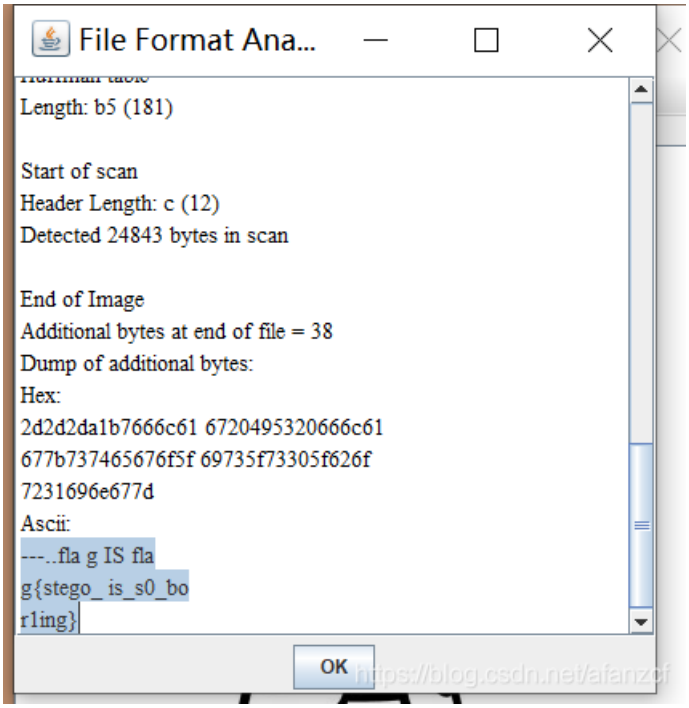


（2）解法二（Stegsolve）

用Stegsolve打开图片，



然后用这个打开。

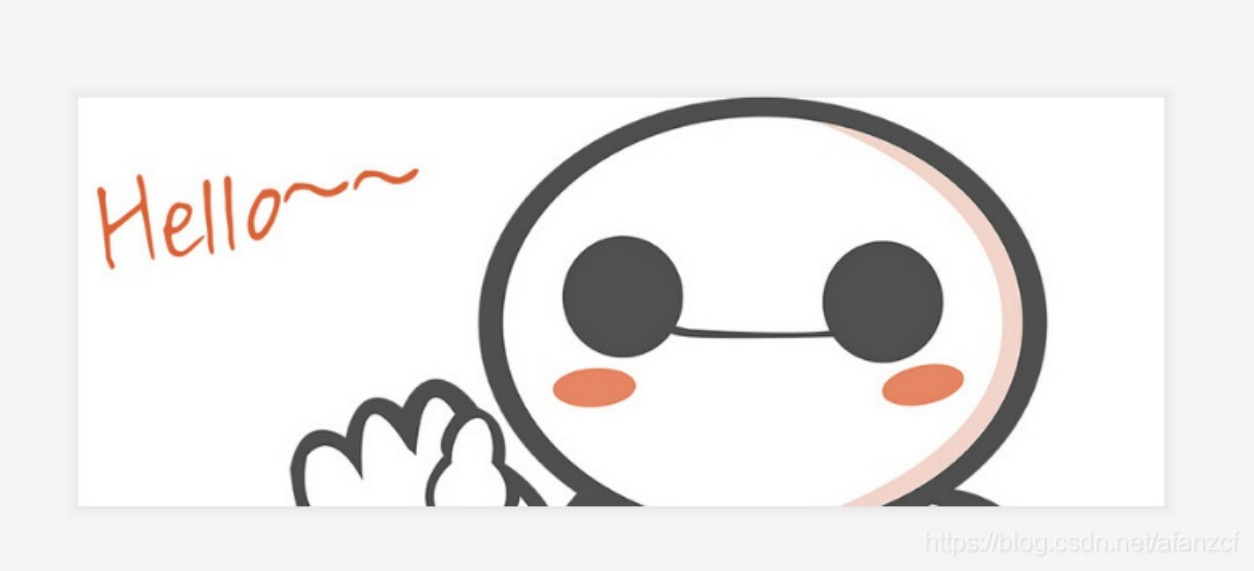


得到flag。

6、大白（winhex修改图片的高度）

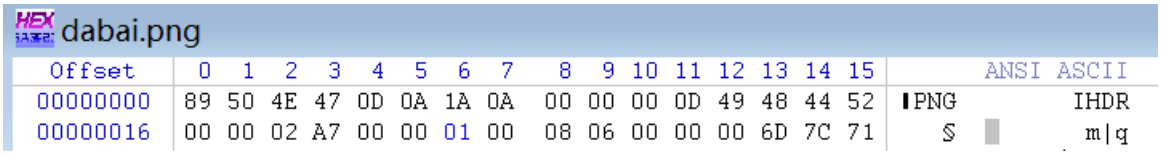
首先看到图片，便知道，这可能是一道修改图片高度的题目。

打开文件一看，果然如此。

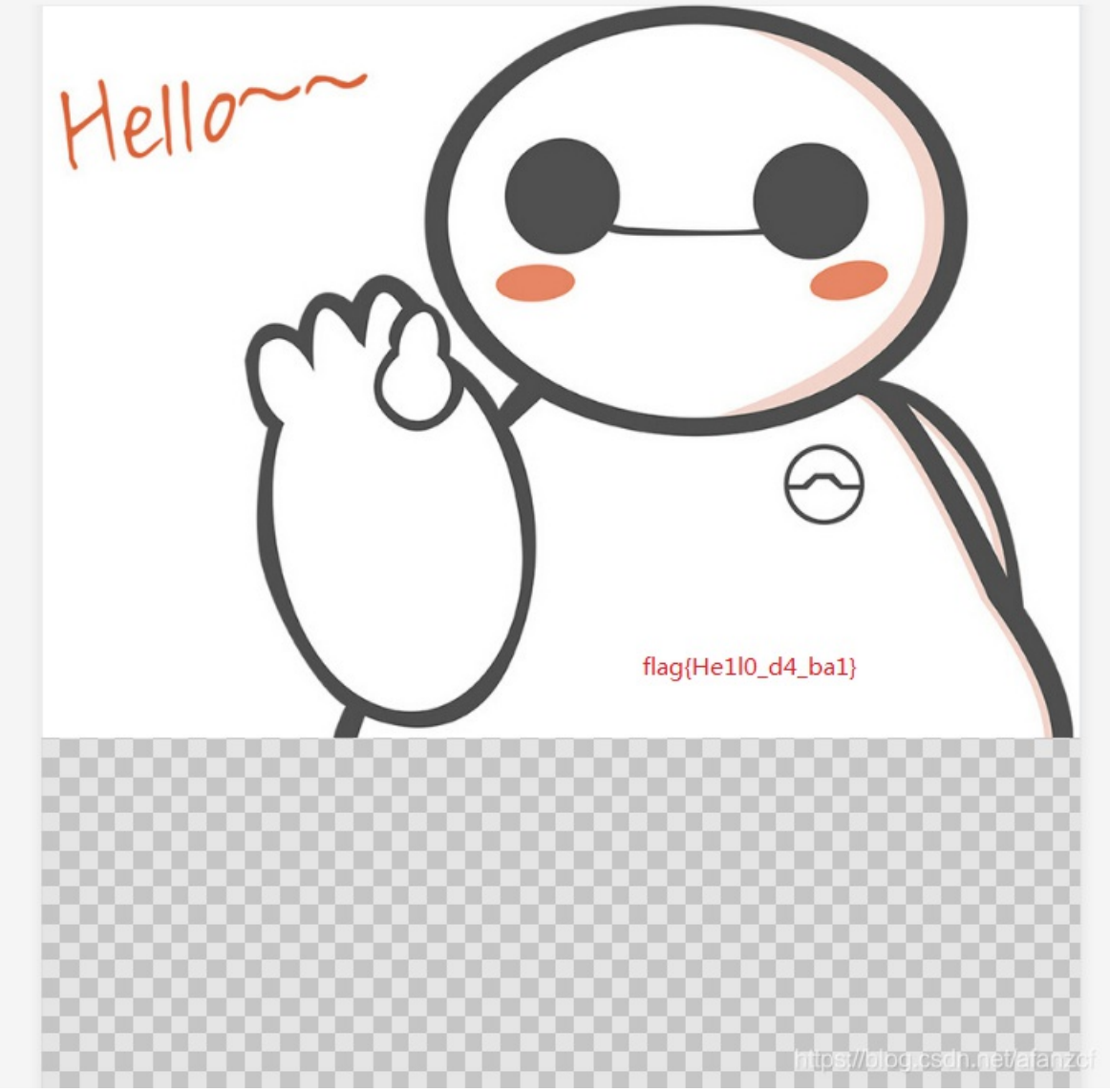


可以看出图片，还有一大截没有露出来。拖入winhex中。

第一行是文件头，第二行的前四个字节是图片的宽度，后面的四个字节是图片的高度。



将01改为A7.保存更新之后，得到falg



flag{He1l0_d4_ba1}

7、基础破解（ARCHPR、base64解密）

从题目看来，应该是要暴力破解了，且密码是4位数字。

打开ARCHPR，暴力破解。

得到解压密码，2563.

ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=

给的txt，一看就是base64了，直接解密。

Base64 在线编码解码 | Base64 加密解密 - Base64.us

Base64.us Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=

编码 (Encode) 解码 (Decode) ↕ 交换 (编码快捷键: Ctrl + Enter)

Base64 编码或解码的结果:

flag{70354300a5100ba78068805661b93a5c}

得到flag。

flag{70354300a5100ba78068805661b93a5c}

8、BUUCTF misc第八题（winhex、Stegsolve）

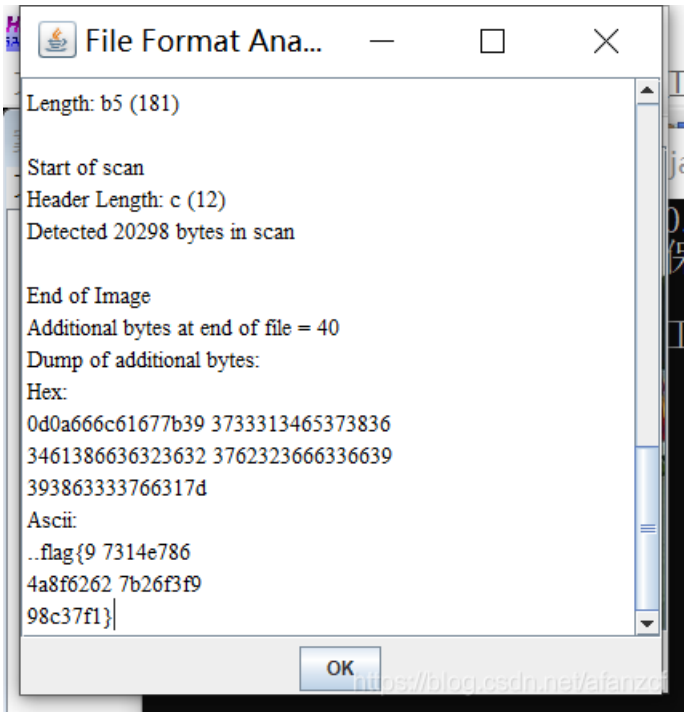
下载之后，又是一个jpg，同5、你竟然赶我走的解法一样。

（1）winhex直接拖到尾

00020752	98	1D	69	AA	AC	BC	97	C0	27	00	1A	9E	24	12	0D	CD
00020768	C9	A9	36	81	8E	FF	00	5A	A0	20	F9	FB	50	65	20	E0
00020784	A9	AB	48	8A	D8	24	75	A1	E1	41	CD	02	2A	34	83	A7
00020800	AF	4A	68	5C	FC	C4	55	B1	04	64	72	29	8D	02	2E	76
00020816	E4	7D	0D	00	45	E5	AB	75	03	F9	51	E5	11	F7	5D	C7
00020832	E3	9F	E7	48	46	D6	1C	E7	9A	90	75	EA	69	01	13	47
00020848	29	18	0E	BF	5C	73	FF	00	EB	A5	43	E5	61	42	90	3D
00020864	73	9A	94	8E	BC	9A	6B	A8	A1	6E	04	72	4C	81	09	67
00020880	0A	07	AD	50	03	32	34	99	E5	CF	4C	F0	3E	95	66	55
00020896	06	5C	1E	8A	38	15	16	C5	DD	D3	1F	4A	D1	20	1F	9F
00020912	7A	29	DE	5A	FB	D1	4F	51	1F	FF	D9	0D	0A	66	6C	61
00020928	67	7B	39	37	33	31	34	65	37	38	36	34	61	38	66	36
00020944	32	36	32	37	62	32	36	66	33	66	39	39	38	63	33	37
00020960	66	31	7D													

00020752	▌	i	ª	¬	¼	▌	À	'		▌	$		İ			
00020768	É	©	6		▌	ÿ		Z		ù	û	P	e		à	
00020784	©	«	H	▌	Ø	$	u	¡	á	A	Í		*	4	▌	§
00020800	¯	J	h	\	ü	Ä	U	±		d	r	)			.	v
00020816	ä	}		E	å	«	u		ù	Q	å		÷	]	Ç	
00020832	ã	▌	ç	H	F	Ö		ç	▌		u	ê	i		G	
00020848	)		¿	\	s	ÿ		ë	¥	C	å	a	B		=	
00020864	s	▌	▌	¼	▌	k	¨	i	n		r	L		g		
00020880				-P		2	4	▌	å	Ï	L	ð	>	▌	f	U
00020896		\		▌	8		Å	Ý	Ó		J	Ñ		▌		
00020912	z	)	Þ	Z	û	Ñ	O	Q		ý	Ù			f	l	a
00020928	g	{	9	7	3	1	4	e	7	8	6	4	a	8	f	6
00020944	2	6	2	7	b	2	6	f	3	f	9	9	8	c	3	7
00020960	f	1	}													

（2）Stegsolve



flag{9 7314e7864a8f6262 7b26f3f998c37f1}

9、BUUCTF 第九题LSB(Stegsolve、QR Research)

下载附件之后，打开是一个png图片，拿到图片之后，打开winhex，发现文件头89504E47，正确，文件尾，AE426082，正确。而且没有在winhex中直接发现flag。于是用Stegsolve打开，查看文件信息，也没有发现flag。

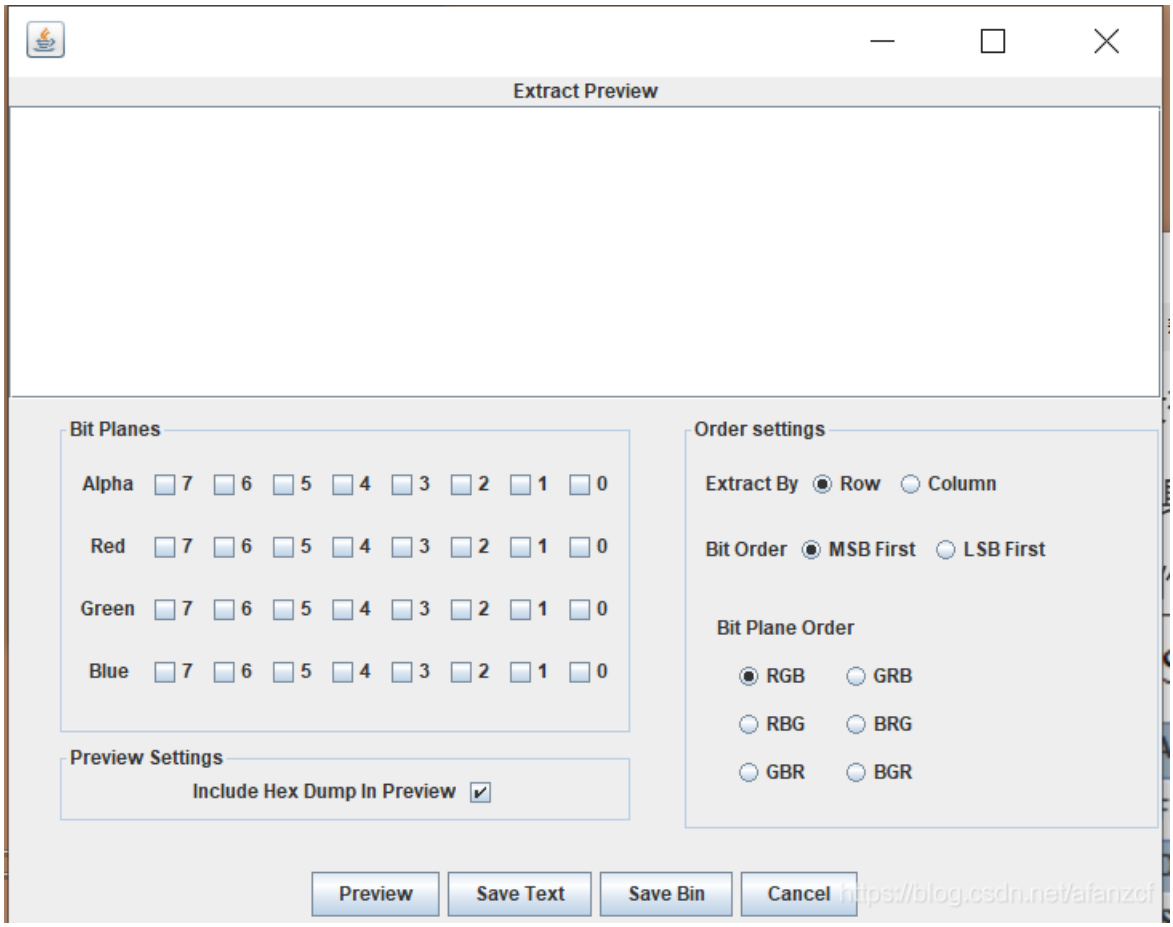
然后怀疑是不是把图片的宽和高修改了，于是在winhex中，找到第二行，修改宽和高，保存之后，直接图片打不开了。。。

常规的图片题，如今方法都失败了，也没有查到在图片里面有其他文件。

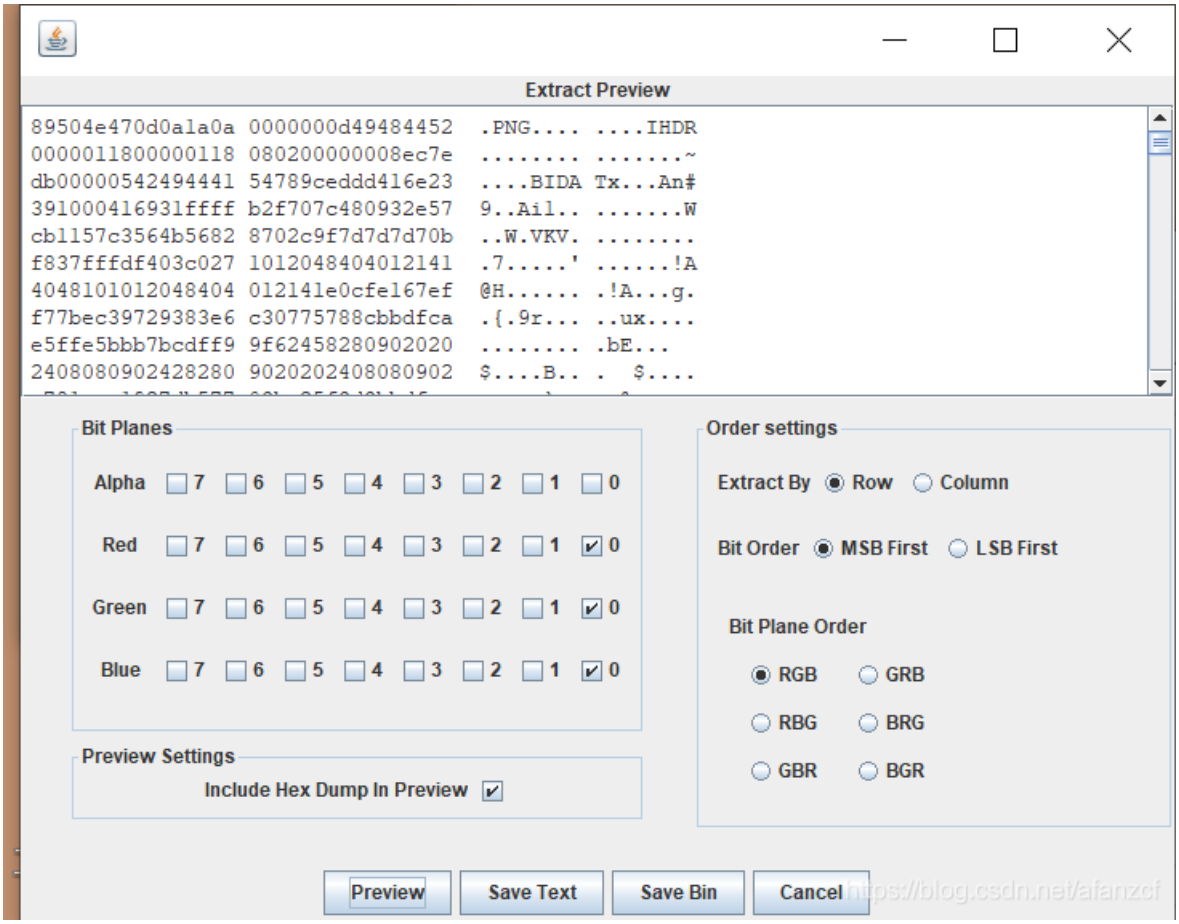
用了Stegsolve的分离图片功能，但是我是一个一个勾选的，且没有注意分离出来的信息。

借鉴了一下wp，发现自己在Stegsolve工具上漏了一个功能。

DATA分离的那个（这里本来有一张图的，但是审核多次不通过，说我政治的问题，想不明白）



打开之后，发现有几个颜色通道。



三个都选了之后，Preview，拖到最上面，发现了有一个信息是png。也就是说，隐藏着一张图片了。

直接保存为xxx.png。然后打开，发现是一张二维码图片。

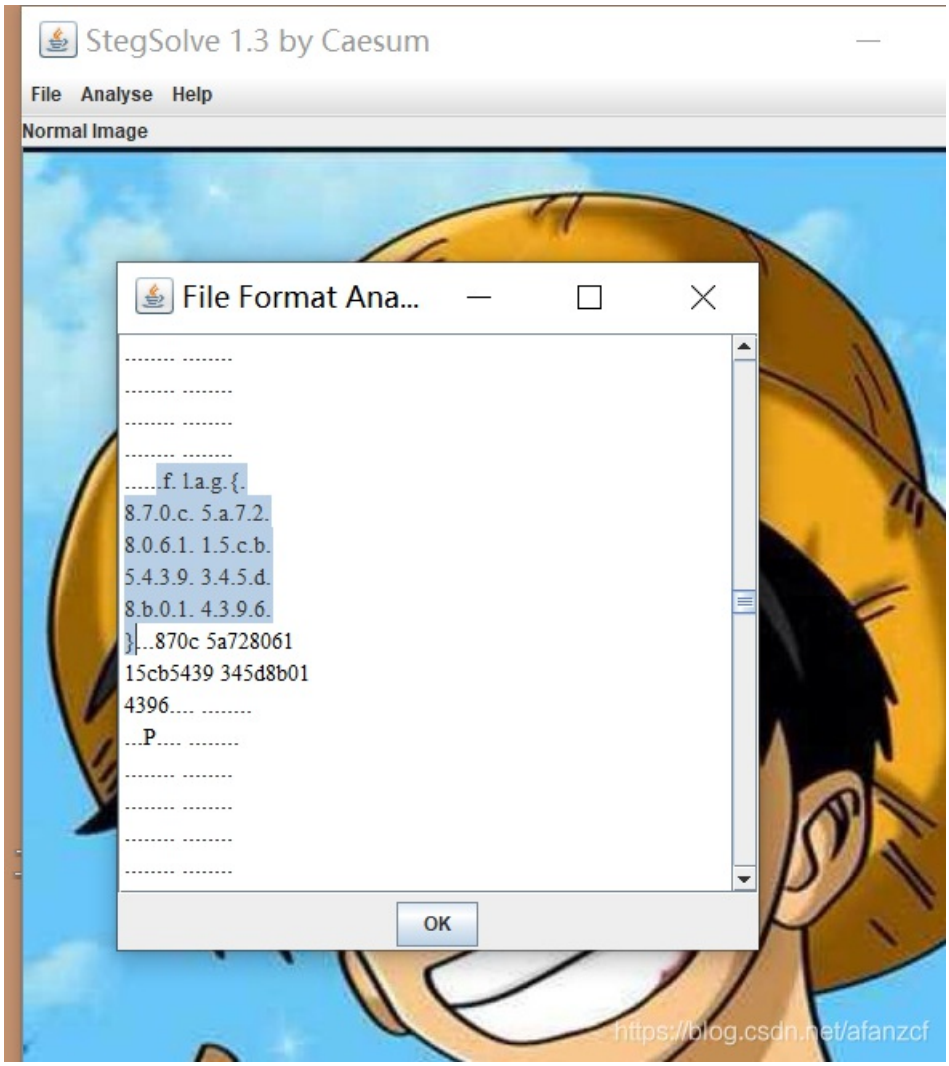
用QR Research扫一下，就得到了flag。

flag{1sb_i4_s0_Ea4y}

10、文件中的秘密（Stegsolve、winhex）

（1）方法一（Stegsolve）

直接打开文件之后，发现是一张jpeg的图片。话不多说，直接用Stegsolve打开图片。

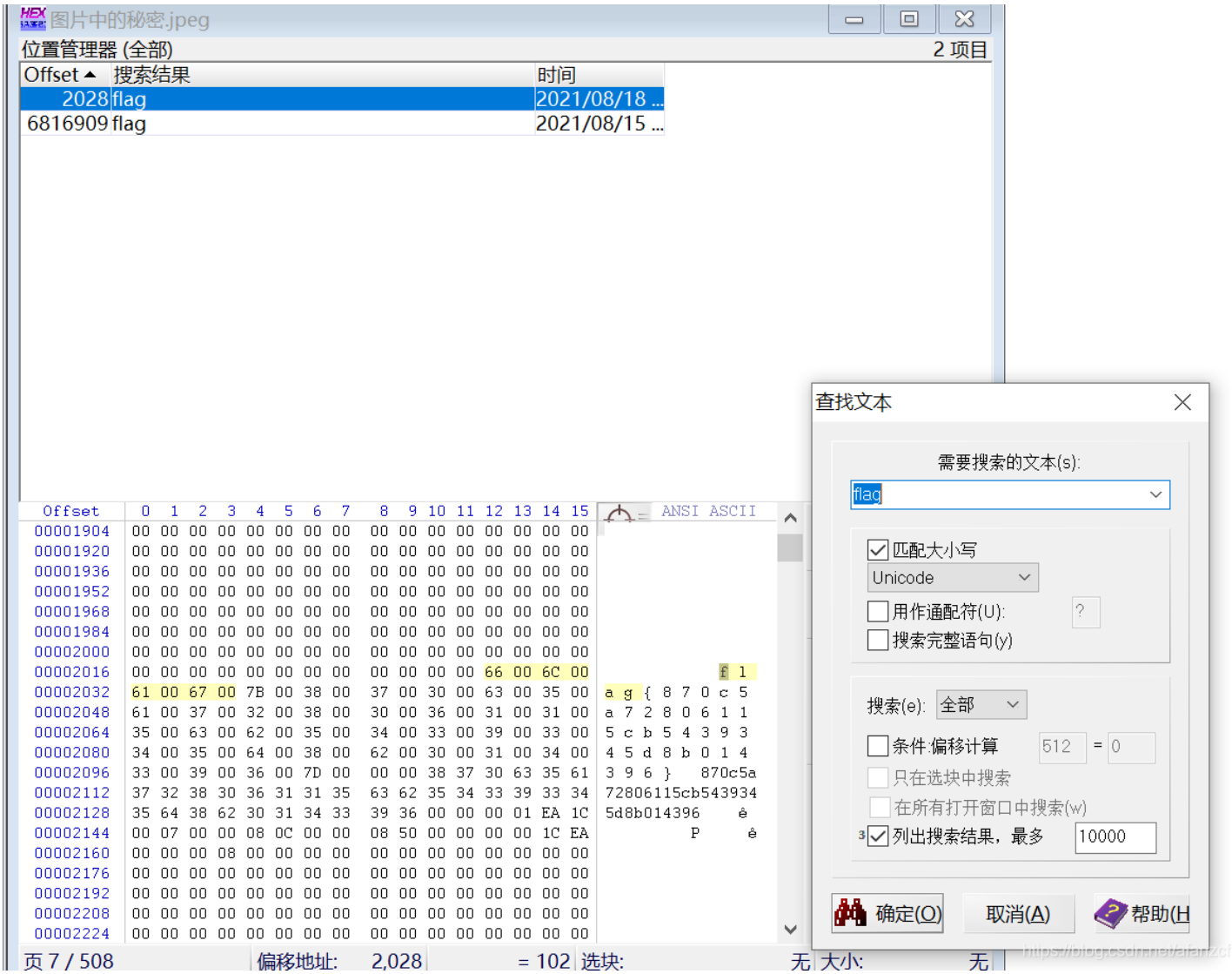


在查看图片具体信息的中间的位置，发现了flag。复制出来之后，将中间的.删去。

得到flag。

flag{870c5a72806115cb5439345d8b014396}

（2）方法二（winhex）



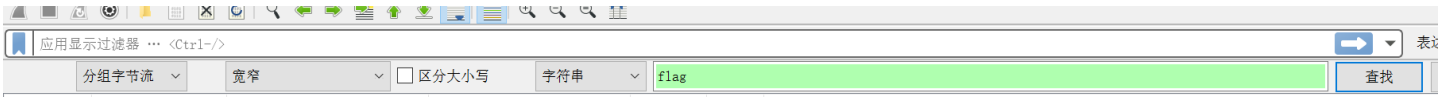
直接winhex里面文本搜索flag。得到flag。

11、wireshark（wireshark）

下载附件之后，是一个pcapng文件，用wireshark打开。

由于目前做这种流量包的题，我就一种方法，搜索字符串。

所以直接搜索字符串flag。



直接查找到flag。

```
> Transmission Control Protocol, Src Port: 22494, Dst Port: 80, Seq: 1, Ack: 1,
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  v Form item: "email" = "flag"
      Key: email
      Value: flag
  > Form item: "password" = "ffb7567a1d4f4abdffdb54e022f8facd"
  > Form item: "captcha" = "BYUG"
```

```
02a0  31 61 37 33 32 64 65 61  35 39 37 61 35 65 63 39   1a732dea 597a5ec9
02b0  34 63 3d 31 34 33 35 35  39 30 35 37 34 0d 0a 43   4c=14355 90574··C
02c0  6f 6e 6e 65 63 74 69 6f  6e 3a 20 6b 65 65 70 2d   onnectio n: keep-
02d0  61 6c 69 76 65 0d 0a 43  6f 6e 74 65 6e 74 2d 54   alive··C ontent-T
02e0  79 70 65 3a 20 61 70 70  6c 69 63 61 74 69 6f 6e   ype: app lication
02f0  2f 78 2d 77 77 77 2d 66  6f 72 6d 2d 75 72 6c 65   /x-www-f orm-urle
0300  6e 63 6f 64 65 64 0d 0a  43 6f 6e 74 65 6e 74 2d   ncoded·· Content-
0310  4c 65 6e 67 74 68 3a 20  36 35 0d 0a 0d 0a 65 6d   Length:  65····em
0320  61 69 6c 3d 66 6c 61 67  26 70 61 73 73 77 6f 72   ail=flag &passwor
0330  64 3d 66 66 62 37 35 36  37 61 31 64 34 66 34 61   d=ffb756 7a1d4f4a
0340  62 64 66 66 64 62 35 34  65 30 32 32 66 38 66 61   bdffdb54 e022f8fa
0350  63 64 26 63 61 70 74 63  68 61 3d 42 59 55 47      cd&captc ha=BYUG
```

可以看到，email = flag，password = ffb7567a1d4f4abdffdb54e022f8facd

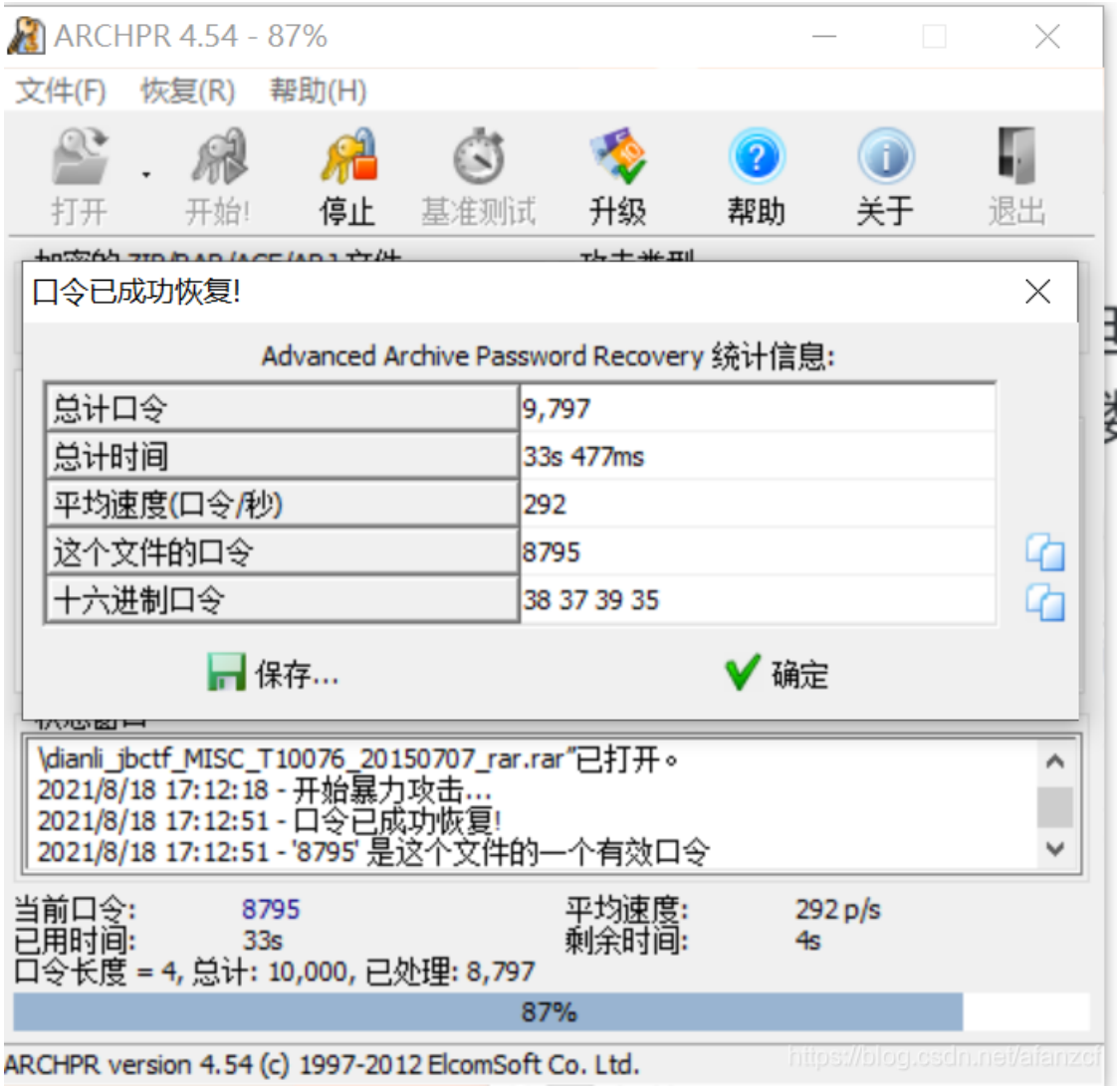
我们就得到了

flag{ffb7567a1d4f4abdffdb54e022f8facd}

12、rar（ARCHPR）

首先看到提示信息。

提示的太明显了。秘密是四位的纯数字，那么直接暴力破解。



压缩包秘密，8975得到

解压。直接就是flag.txt。打开就是flag

flag{1773c5da790bd3caff38e3decd180eb7}

总结

花了一个上午和下午的时间，做完了这十二道题，随着在攻防世界 新手练习区Misc的经验积累，以及自己对很多工具的了解之后，做这十二道题，倒也是比较轻松了。从这十二道题来说，大部分题目是跟图片有关的，

（1）跟图片有关，那么两个工具，

一个是winhex，一个是Stegsolve，首先问winhex看看，图片里面有没有被隐写其他的文件，然后如果感觉图片的宽高被改写，那么使用winhex直接改写，还有就是有的题目，直接将flag写在了图片中，在winhex中直接搜索flag即可，或者使用Stegsolve的查看信息功能，查看也行。

（2）如果是跟rar，zip有关，

根据题目告诉的密码提示，直接使用工具暴力破解密码即可，虽然现在大部分密码还是四位数的简单密码，但是至少在脑海中，也是要有这个思路才行。

（3）还有一个题倒是需要使用wireshark工具，

但是也还算是简单题目，直接搜索字符串flag就行，之前在攻防世界遇到一个wireshark的题目，是在搜索flag之后，查找到了其他几个文件，比如xxx.txt，xxx.jpg，这时候就需要先使用foremost先分离文件之后，再解题了。

这是目前我所遇到的Misc题目的一些思路，随着自己的做题，后面遇到的题目和脑洞也会越来越大，继续加油啊。