

# BUUCTF\_MISC题解

原创

[TYUT\\_网安小菜鸡](#) 于 2021-05-30 22:12:54 发布 1942 收藏 24

分类专栏: [BUUCTF](#) 文章标签: [信息安全](#)

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/m0\\_52885531/article/details/117406720](https://blog.csdn.net/m0_52885531/article/details/117406720)

版权



[BUUCTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

## BUUCTF\_MISC题解

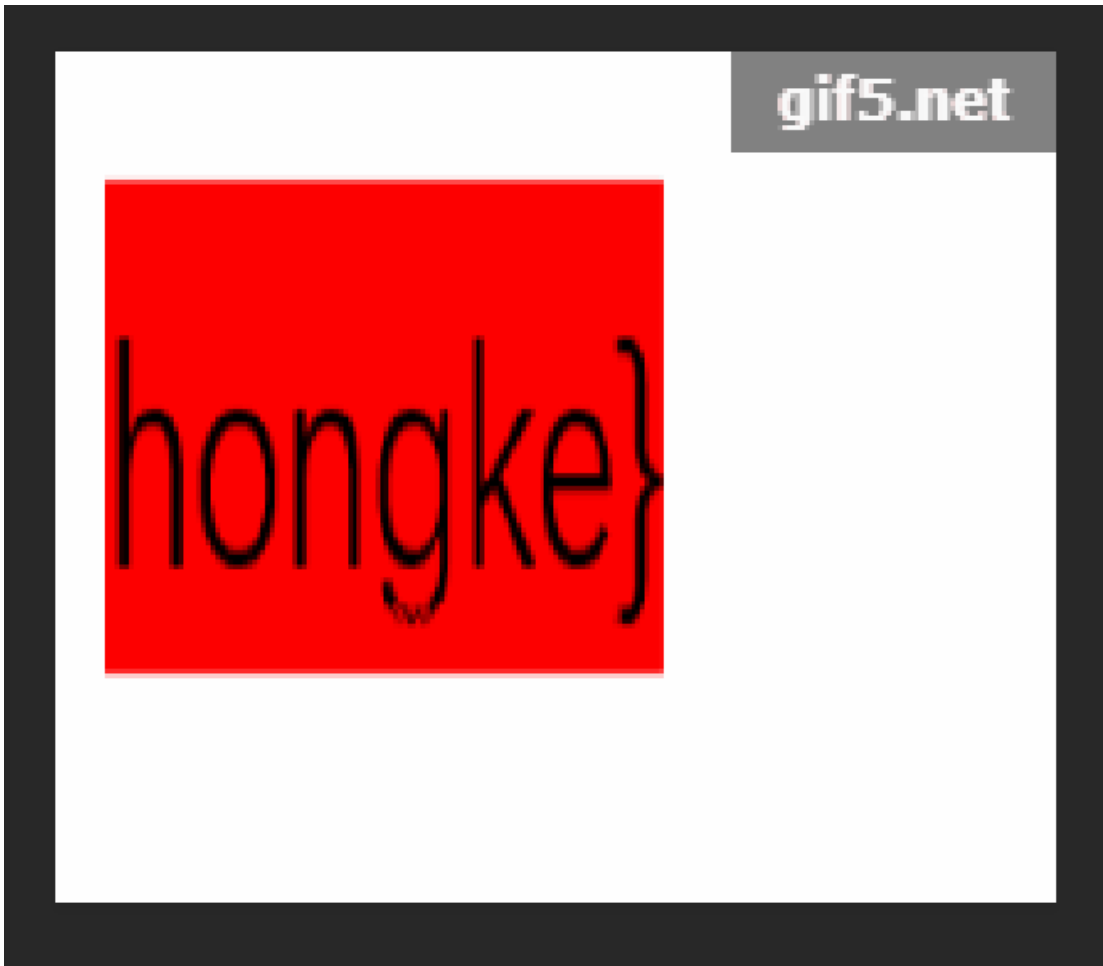
### 第二题

将GIF图片用ps进行逐帧分解, 可以得到三张特殊的照片



gif5.net


he11o



直接将三个照片里的内容拼接起来就好

### 第三题 二维码

下载好附件解压后发现是一个.png文件的二维码

 QR_code.png	2018/11/6 18:07	PNG 文件	1 KB
--	-----------------	--------	------

用CQR扫描后得到二维码的结果

```
已解码数据 1:
-----
位置:(10.3,10.3)-(268.4,10.3)-(10.3,268.4)-(268.7,268.7)
颜色正常, 正像
版本:2
纠错等级:H, 掩码:7
内容:
secret is here
-----
```

发现并没有得到想要的flag，并且提示我们flag并不在这李，那我们就用二进制编辑器打开看一看在哪里。

```
8B 7E 01 B2 1B 8D D5 E6 69 67 86 00 00 00 00 49 .~.....ig....l
45 4E 44 AE 42 60 82 50 4B 03 04 14 00 09 00 08 END B`.PK.....
00 8B 50 2F 48 46 34 4C AE 1D 00 00 00 0F 00 00 ..P/HF4L.....
```

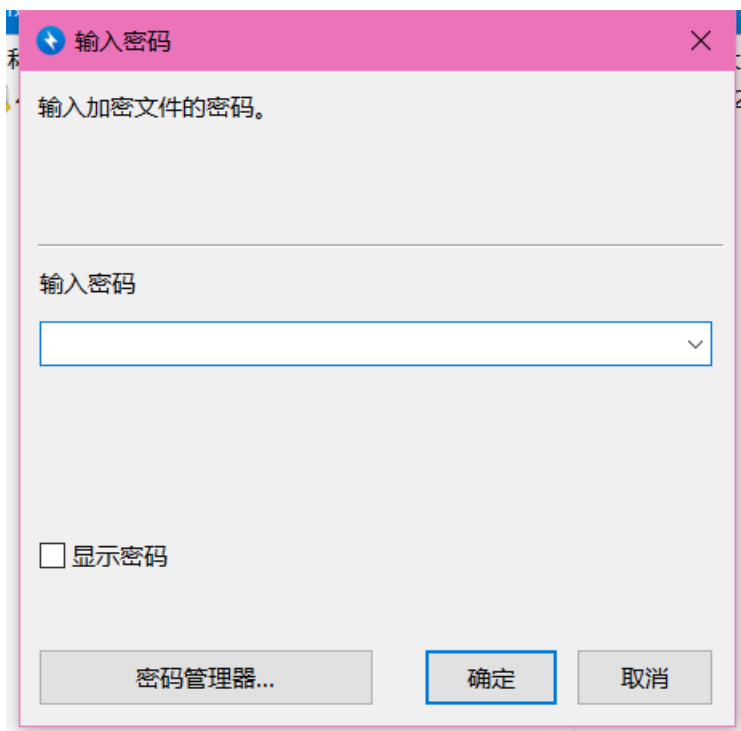
.png的文件尾是AE 42 60 82，按理来说在文件尾之后就应该结束，我们却发现png的文件尾后还跟着50 4B 03 04，这是.zip的文件头，说明在该照片下还隐藏着一个.zip文件，到这一步有两种方法：

1. 将50 4B 03 04之前的东西全部删掉，之后保存，将文件后缀名改为.zip
2. 用Linux中的binwalk将隐藏的.zip文件分离出来。语句：binwalk -e 文件名

然后打开这个.zip文件，解压它，但是！它居然加密了，我们看看是不是伪加密

伪加密这里可以看这个大佬的文章学习

[https://blog.csdn.net/qq\\_26187985/article/details/83654197](https://blog.csdn.net/qq_26187985/article/details/83654197)



再用二进制编辑器打开这个.zip文件

```
EA 01 CD 7F AD 4F 50 4B 07 08 40 34 4C AE 1D 00 .....PK..F4L...
00 00 0F 00 00 00 50 4B 01 02 1F 00 14 00 09 00 .....PK.....
08 00 8B 50 2F 48 46 34 4C 4F 1D 00 00 00 0F 00 ..P/HF4L
```

发现核心目录区头504B0102四个bytes之后的数为：09 00，而不是00 00，说明这个.zip文件加密方式是全局真加密，我们只能去找密码了。可以看见压缩包内的.txt文件名为4numbers，说明密码是四位数字，那我们用kali自带的fcrackzip进行弱口令爆破就行，语句为：fcrackzip -b -c1 -u -l4 文件名

```
root@kali2020:~/桌面# fcrackzip -b -c1 -u -l4 1D7.zip
```

```
PASSWORD FOUND!!!!: pw = 7639
```

```
root@kali2020:~/桌面#
```

发现密码是7639

ok, 那就打开它

```
CTF{vjpw_wnoei}
```

这样就得到了flag

## 第四题 N种方法解决

下载附件之后发现是一个.exe文件，结果却发现打不开

此应用无法在你的电脑上运行

若要找到适用于你的电脑的版本，请咨询软件发布者。

关闭

那我们就试试拿二进制编辑器打开，看看它是个什么东东

```
KEY.exe x  
data:image/jpeg;base64,iVBORw0KGgoAAAANSUhgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0IArs4c6QAAARnQU1BAACxjwv8YQUAAAJcEhZcw
```

哇哦，发现这个东西一点都不简单，哪是什么.exe文件，分明就是一个.jpg转成了base64，百度一下怎么办，发现只需要把那一行丢到浏览器里打开一下就好。



手机扫一下，得到结果KEY{dca57f966e4e4e31fd5b15417da63269}

## 第五题 大白

这道题目就给了很大的提示

A screenshot of a challenge interface. At the top, there are two tabs: 'Challenge' and 'Top 3 Solves'. The title '大白' is prominently displayed in the center, with a '1' below it. A message reads: '看不到图? 是不是屏幕太小了 注意: 得到的 flag 请包上 flag{} 提交'. Below this is a download button with a file icon and the text '379140b0-c...'. At the bottom, there is a 'Flag' input field and a 'Submit' button.

说明照片中是隐含了消息的，只不过不是我们屏幕太小看不见，而是它通过更改照片的尺寸给隐藏起来了

我们继续用二进制打开这个.png文件

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 .PNG.....IHDR
00 00 02 A7 00 00 01 00 08 06 00 00 00 6D 7C 71 .....m̂q
```

这里有一个知识点

用二进制打开的.png文件的第二行中，前四位表示的是宽度，后四位表示的是长度

我们将其进行修改

```
89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 .PNG .....IHDR  
00 00 02 A7 00 00 02 A7 08 06 00 00 00 6D 7C 71 .....nHQ
```

将其都修改成00 00 02 A7，再次打开照片就得到了想要的东西



## 第六题 你竟然赶我走？

这道题比较简单

我们直接拿二进制编辑器打开这个.jpg文件，而在它的最底部就写着flag

```
40 05 14 51 40 05 14 51 40 1F FF D9 2D 2D 2D A1 @. Q@. Q@. . ---.
B7 66 6C 61 67 20 49 53 20 66 6C 61 67 7B 73 74 . flag | S flag{ st
65 67 6F 5F 69 73 5F 73 30 5F 62 6F 72 31 69 6E ego_i s_s0_bor1i n
67 7D g} ←
```

## 第七题 基础破解

Challenge Top 3 Solves ×

# 基础破解

## 1

给你一个压缩包，你并不能获得什么，因为他是四位数字加密的哈哈哈哈哈。。不对= =我说了什么了不得的东西。。注意：得到的flag请包上flag{}提交

📄 5e46643e-b...

Flag Submit

题目给了我们很大的提示：这是一个加密过的.rar文件，并且密码是四位数字。

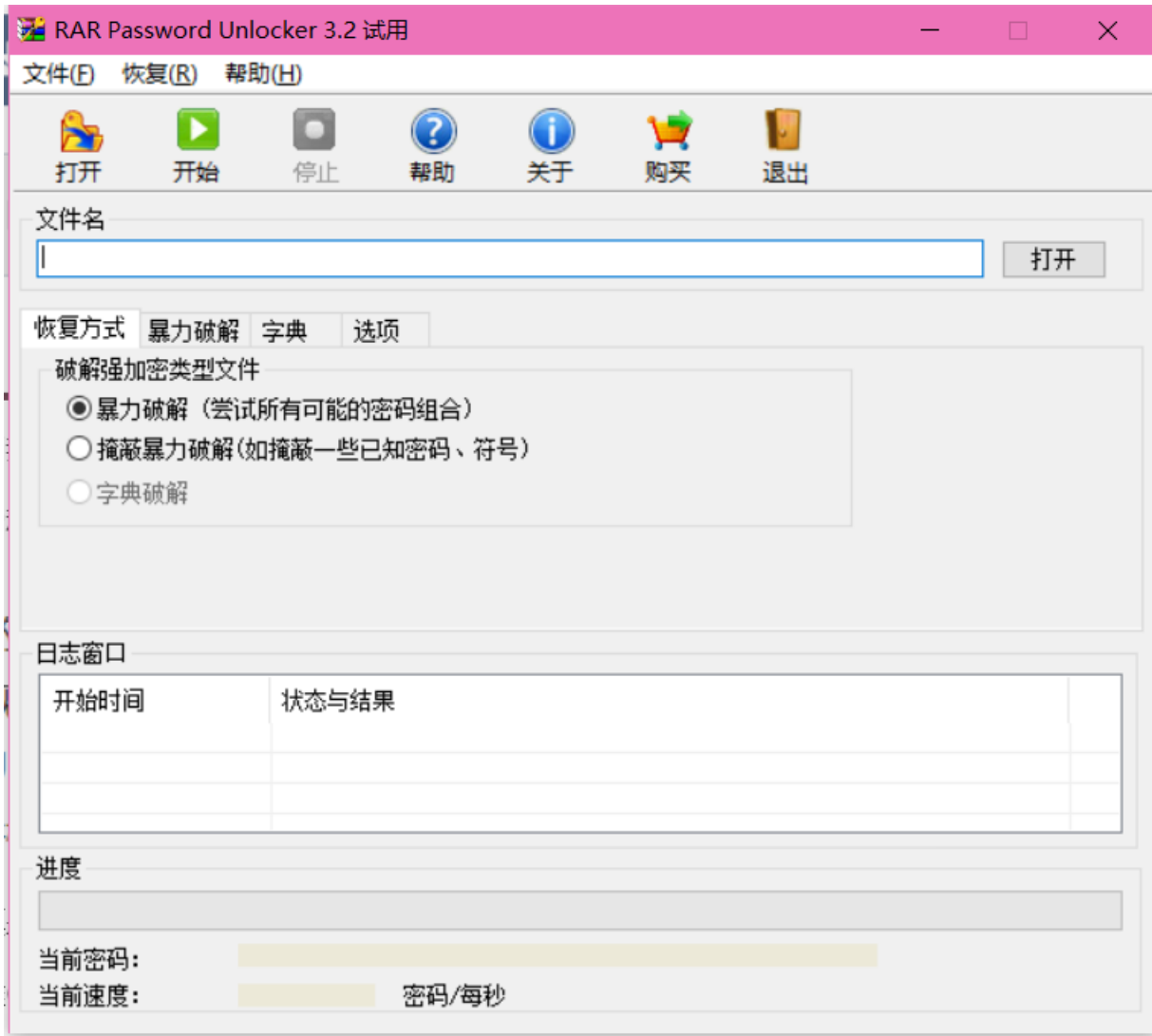
本来以为和第三题一样用fcrackzip爆破，结果fcrackzip只能爆破.zip文件，那就百度一下吧

上网的过程中经常会碰到下载的rar压缩文件有密码,或者自己很久以前为了安全而加密的重要文件。现在忘记了密码需要暴力解的情况,今天我就专门教大家使用一个非常简单的工具RARPassword Unlocker 3.2绿色版,这个软件不用注册,而且是免费的,一分钟就可以学会哦。不过只针对RAR文件格式的密码破解,zip、7z等的格式不支持哦。

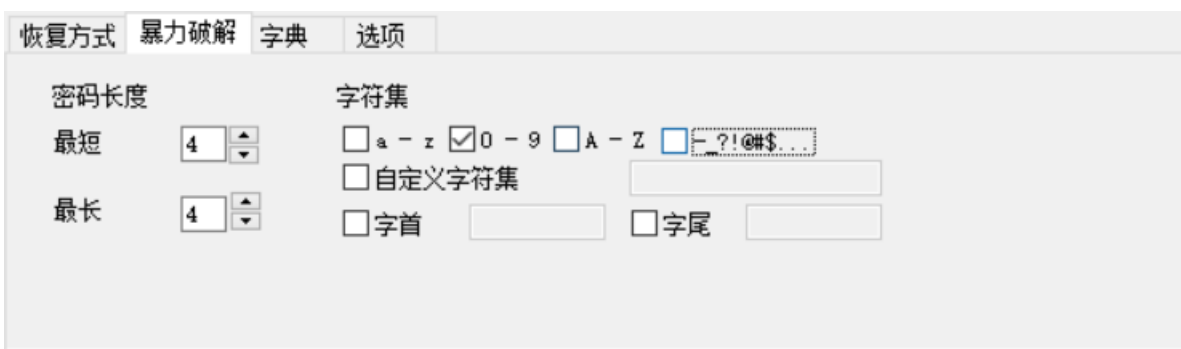
百度可真是个好东西

刚好一堆CTF工具合集里有RARPassword Unlocker 这个软件，那就试试

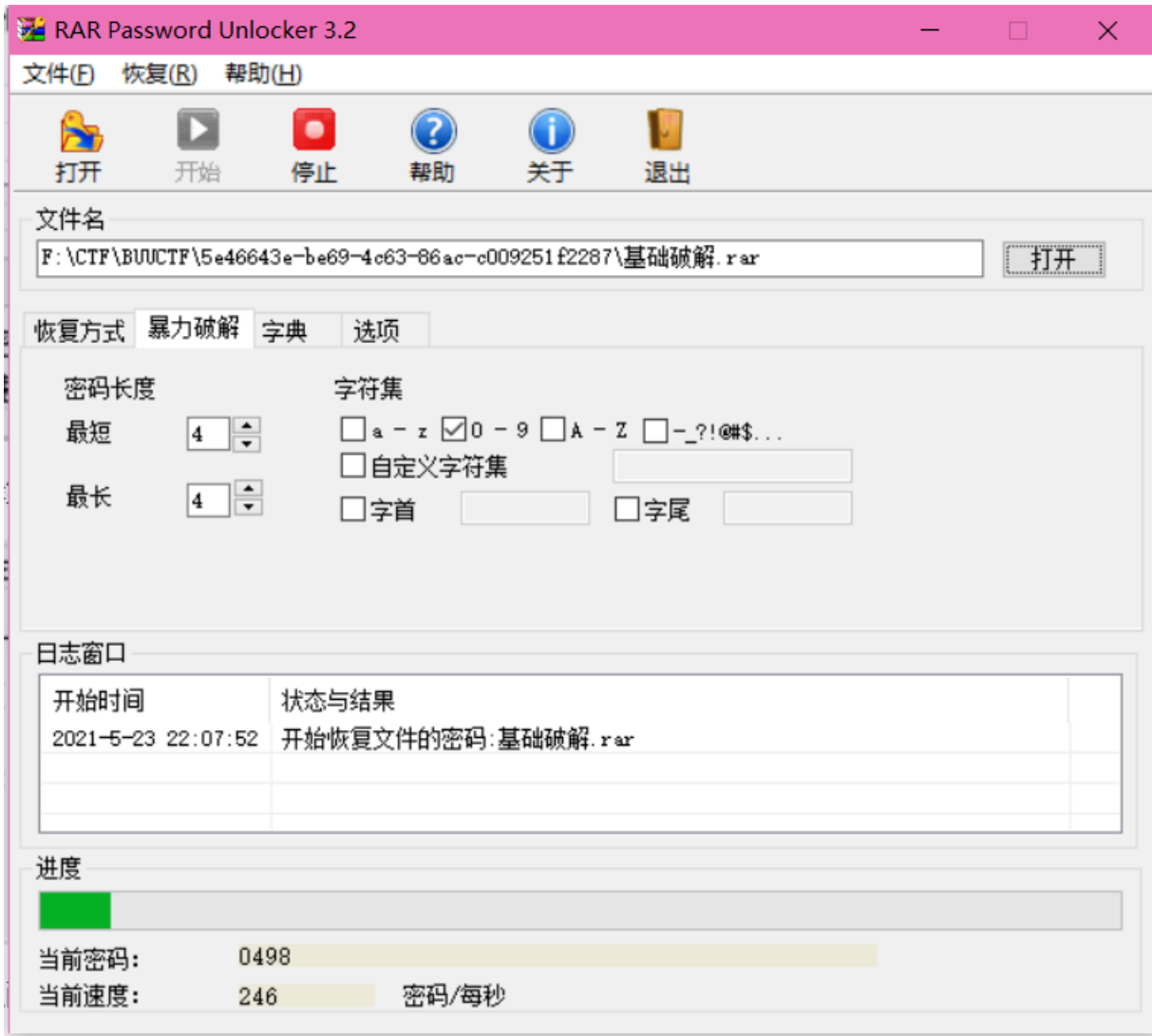




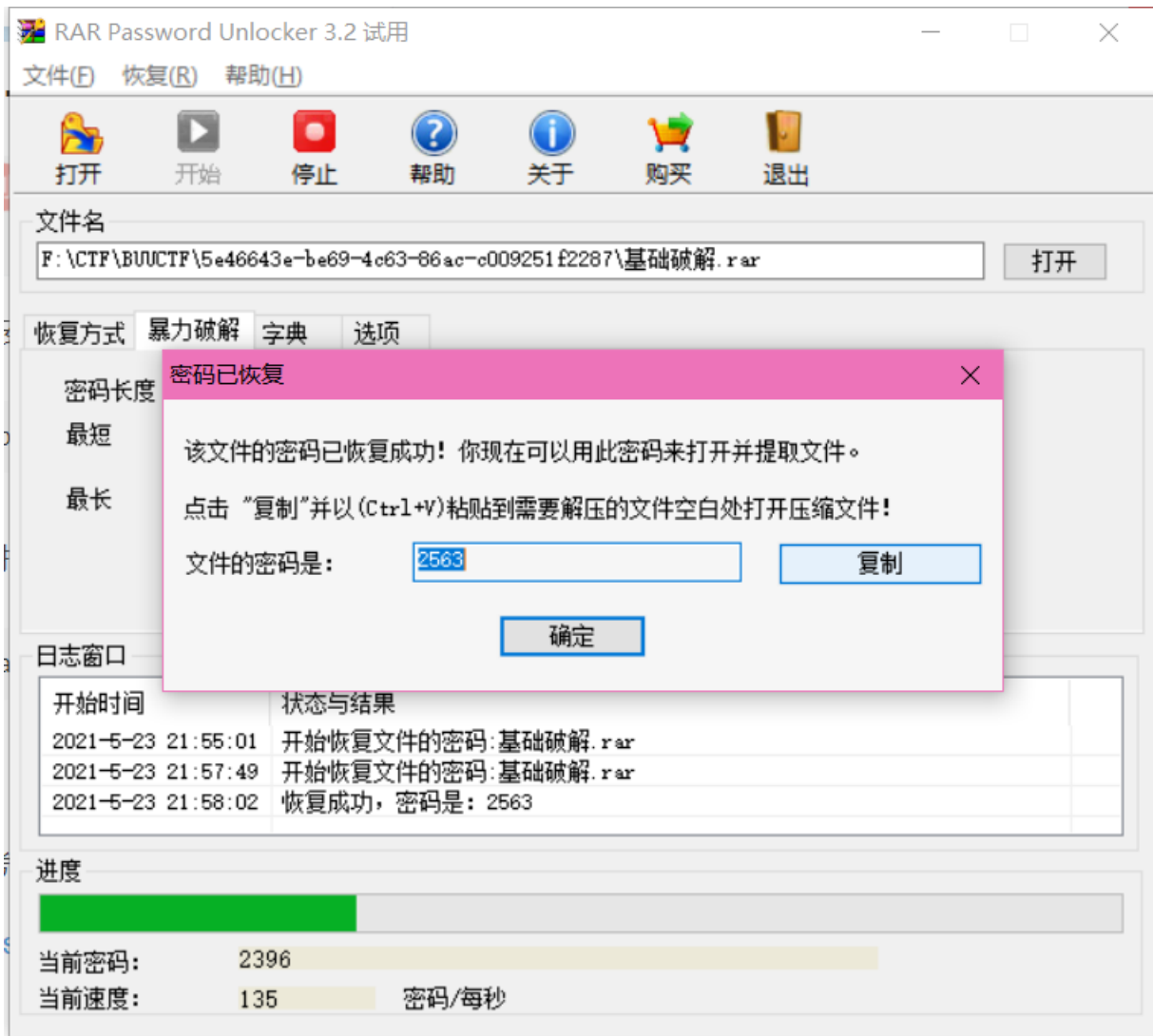
我们选择第二个掩蔽暴力破解，因为我们已经知道密码是四个数字了



我们这么配置一下，然后让它去跑一下



这是跑起来的样子



然后就跑到了密码: 2563

解压!

打开那个flag.txt

```
1 ZmxhZ3s3M0M0M1NDMwMGE1MTAwYmE3ODAzODgwNTY2M0I1M2E1Y30=
```

很显然使用base64加密的一段文字, 俺们去在线解密一下

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**)

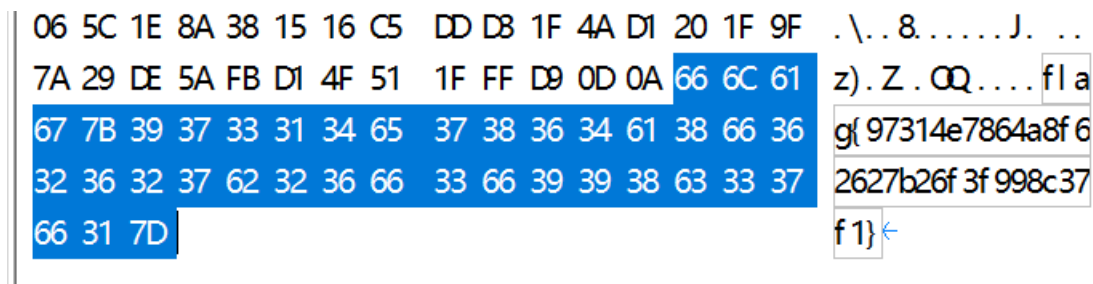
Base64 编码或解码的结果:

flag{70354300a5100ba78068805661b93a5c}

一不小心就得到了flag

## 第八题 乌镇峰会种图

下载附件之后是一个.jpg文件，观察照片里并没有什么有用的信息，还是老思路，用二进制编辑器打开，看看有没有藏什么信息



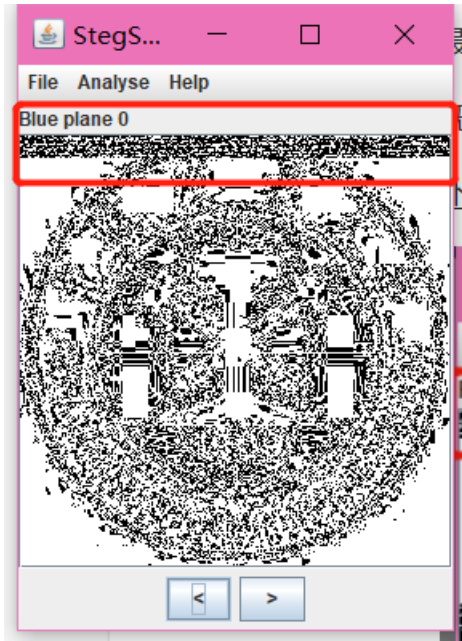
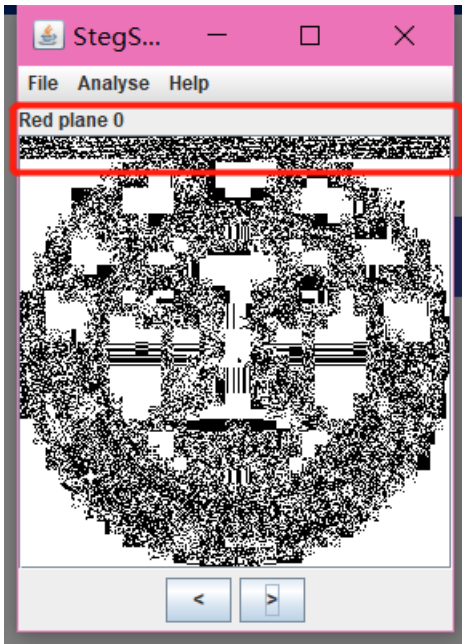
事情就是如此的巧妙

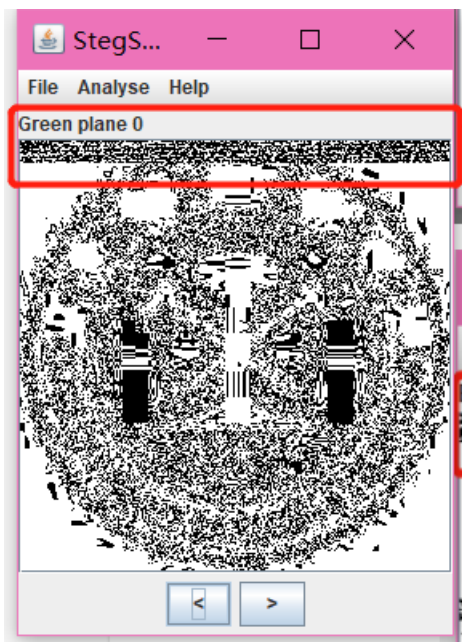
## 第九题 LSB

题目给的信息很清楚LSB，也就是Least Significant Bit（最低有效位）。在大多数PNG图图像中，每个像素都由R、G、B三原色组成，每种颜色一般用8位数据表示，如果修改其最低位，人眼是不能区分出这种微小的变化的，因此可以利用每个像素的R、G、B颜色的分量的最低有效位来隐藏信息，这样每个像素可以携带3位的信息。（摘编自c0d1\_CTFer）

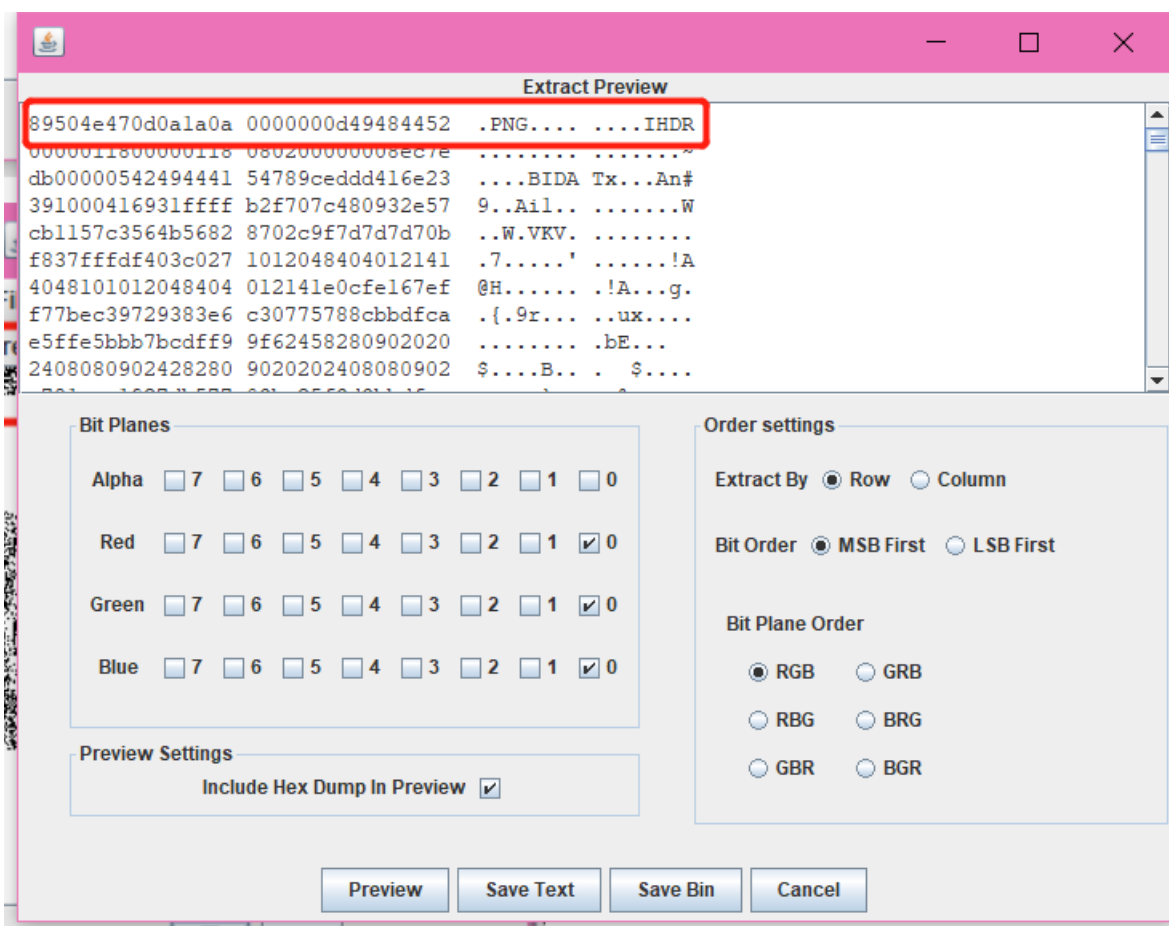
既然题目给的信息这么明显，那我们直接就按LSB来处理信息。

处理LSB最常用的软件是Stegsolve，我们打开这个.png文件，我们先一个个查看图像





由着三个图片可以看出来，在这三个通道上是隐藏了信息的，具体分析看看是什么信息



可以发现是隐藏了一个.png文件在这里，我们点击Save Bin将这个.png文件保存下来看看是什么结果发现是一个二维码



扫描之后得到了信息



## 第十题 文件中的秘密

下载好附件打开后，发现是一个.jpeg格式的文件，还是老样子用二进制编辑器打开

首先我们就注意到了一点

```

FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 01 ..... JFI F.....
00 01 00 00 FF E1 10 A8 45 78 69 66 00 00 4D 4D | ..... Exif.. M
00 2A 00 00 00 08 00 03 87 69 00 04 00 00 01 .*.....i.....

```

**EXIF**，它是在提示我EXIF吗？？

屏幕前的小伙伴可能没看过c0d1\_CTFer所以这里简单介绍一下



EXIF（可交换图像文件格式）可以用来记录数码照片的属性信息和拍摄数据，EXIF可以被附加在JPEG、TIFF、RIFF等文件中，为其增加有关数码相机拍摄信息的内容。缩略图或图像处理软件的一些版本信息。

所有我们直接用Windows自带的属性打开查看一下



芜湖，一切都是如此的妙不可言

## 第十一题 wireshark

题目提供了很详细的信息：wireshark抓到管理员登录网站的一段流量包（管理员的密码即是答案）

下载好附件后，我们先用wireshark打开这个数据包

ctrl+f调出搜索框，依次选择分组字节流，宽窄，字符串，然后我们进行查找flag

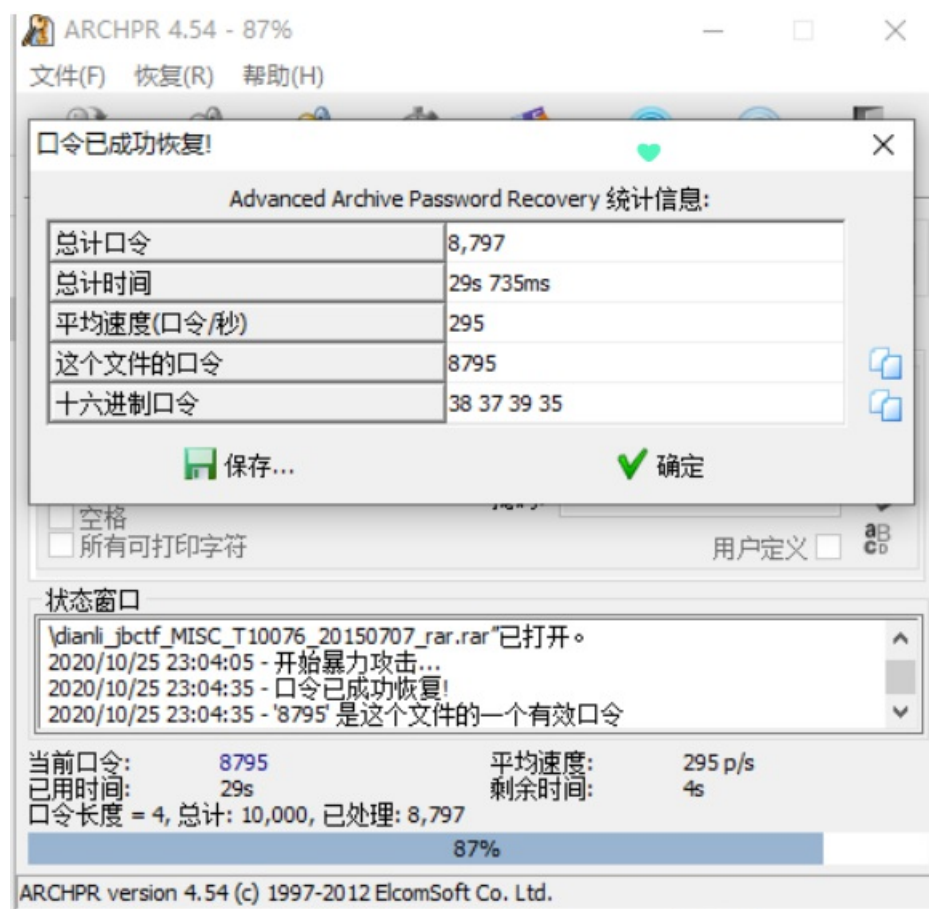


查找后发现结果的第一个数据包就含有flag，而在flag后紧跟着的就是password，这正好与对应，根据题目的指引，那么password里的数据就是flag

```
61 69 6c 3d 66 6c 61 67 26 70 61 73 73 77 6f 72  ail=flag &passwor
64 3d 66 66 62 37 35 36 37 61 31 64 34 66 34 61  d=ffb756 7a1d4f4a
62 64 66 66 64 62 35 34 65 30 32 32 66 38 66 61  bdfdb54 e022f8fa
63 64 26 63 61 70 74 63 68 61 3d 42 59 55 47    cd&captc ha=BYUG
```

## 第十二题 rar

首先看题目提示的很清楚，四个数字密码，而且附件是.rar我们就直接暴力破解密码



8795

输入密码打开后发现一个.txt文件

```
1 |flag{1773c5da790bd3caff38e3decd180eb7}
```

得到了flag

## 第十三题 qr

下载好附件后是一个二维码，扫描之后得到了flag



## 第十四题 zip伪加密

题目告诉我们的信息很少但是已经足够了“zip伪加密”

果不其然,我们在打开附件的时候提示我们输入密码

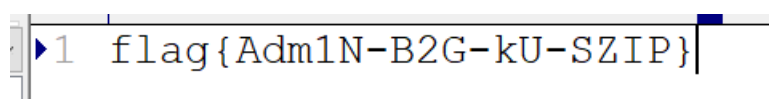
但因为是伪加密,我们也不需要去爆破密码,我们依旧用二进制编辑器打开它

我们找到核心目录其头50 4B 01 02后的8个字节

```
D8 75 32 72 D7 CD 0E D5 0D 8E F2 0C A8 05 00 50 .u2r.....P
4B 01 02 1F 00 14 00 01 00 08 00 50 A3 A5 4A 21 K.....P..J!
```

是01 00 说明这个zip是伪加密,我们只需要将其修改成00 00就解除了它的伪加密,就可以直接打开文件了

得到一个.txt文件,里面就是flag



## 第十五题 ningen

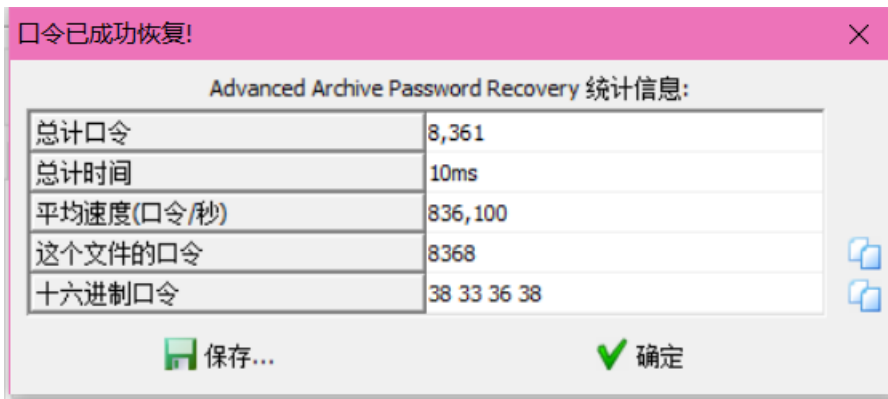
下载好附件之后是一个.jpg格式的文件,我们用二进制编辑器打开它,搜索50 4B 03 04 (这是.zip文件的文件头)

```
D9 50 4B 03 04 14 00 01 00 00 00 D1 7E 96 45 32 .PK.....~E2
0F BA 58 32 00 00 00 26 00 00 00 0A 00 00 00 6E ..X2..&.....n
```

结果不小心发现了这个小东西

那我们就把50 4B 03 04之前的东西全部删掉,然后保存,并将文件名修改成.zip

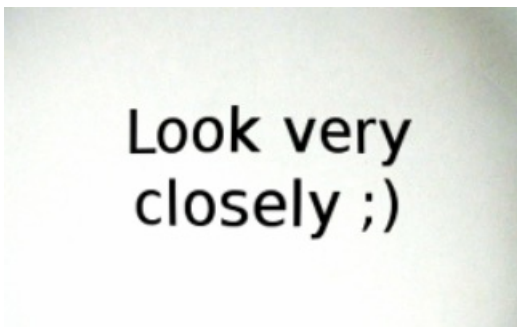
我们将它打开,发现有密码,但是题目告诉了我们这是一个4位数字密码,我们用工具爆破一下



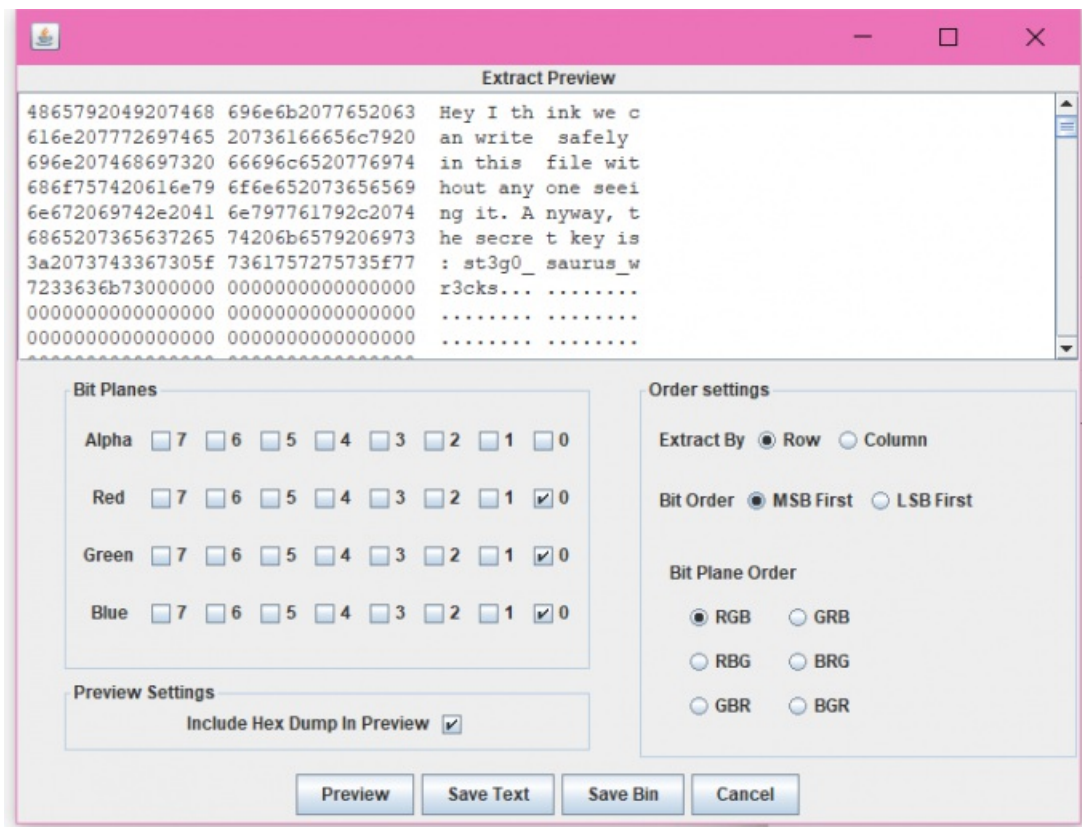
得到了密码，那就解压，打开，之后的我就不详细说明了哦

## 第十六题 镜子里的世界

我们下载好附件以后发现是一个.png文件，用二进制打开观察发现是一个纯纯的.png文件没有夹杂其它别的东西



那我们试试用StegSolve打开它，把所有通道都查看一遍之后没发现任何奇怪的地方，那就具体分析分析他的R、G、B通道的最低有效位，哇哦，一不小心就发现了好东东



## 第十七题 被嗅探的流量

被嗅探的流量，emmmm，很有味道□

用wireshark打开附件，和第十一题的步骤一样，我们在这么多数据包中搜索带有flag字符的

然后第一个包中上传了一个名叫flag的.jpg文件

```

!2 66 6c 61 67 2e 6a 70  filename= "flag.jp
is 6e 74 2d 54 79 70 65  g"··Content-Type
ia 70 65 67 0d 0a 0d 0a  : image/jpeg····

```

我们右键这个数据包，然后追踪它的TCP流，我们在所追踪出的TCP流中再进行查找flag，结果就得到了

```

Q..9...R3.....M.....V.....X.S._x.Z=...XI.....H/.a...
a.....?...J.....flag{da73d88936010da1eeeb36e945ec4b97}.
WebkitFormBoundaryTo8P7n30Ac27kT3U

```

## 第十八题 小明的保险箱

下载好附件之后是一个.jpg文件，但是题目说保险箱有一个四位数的密码，因此我们猜测在这个.jpg文件中肯定还隐藏了其他文件，我们用二进制编辑器打开这个文件。

```

A0 06 F1 9E DD 69 38 F6  FD 69 F4 50 07 FF D9 52 .....i8.i.P...R
61 72 21 1A 07 00 CF 90  73 00 00 0D 00 00 00 00 ar!.....s.....

```

我们发现FF D9就是.jpg的文件尾就应该结束了，可后面还加了52 61 72 21这正是.rar的文件头吗

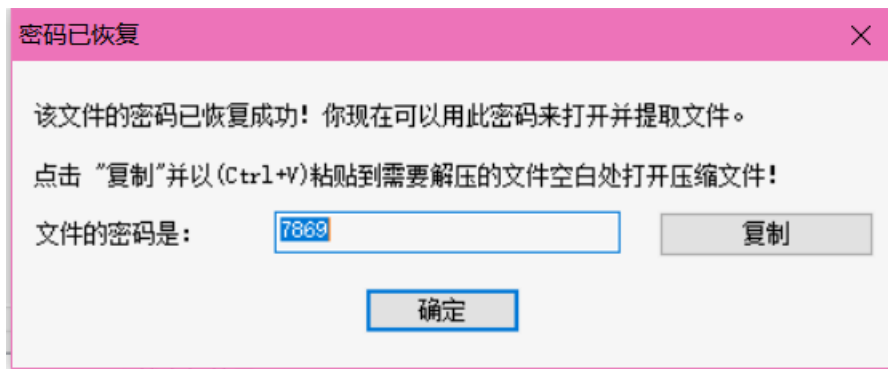
说明这里还藏着一个.rar文件，那就很easy了，还是老规矩，我们把.rar文件分离出来（之前说了太多次怎么分了，这里就不加赘述了）

解压时很自然的发现需要密码，这也很正常，毕竟人家早就告诉你有密码了

我们依旧使用爆破工具进行爆破



设置好之后进行爆破



一不小心就得到了密码

## 第十九题 爱因斯坦

下载好附件后打开发现是一个.jpg文件，用二进制打开，查找.jpg的文件尾FF D9发现在其后面还有一个.zip文件

```
3F FF D9 50 4B 03 04 0A 00 09 00 00 00 A5 2E 61 ?..PK ..... a
47 93 78 C7 0D 33 00 00 00 27 00 00 00 08 00 1C Gx..3...'.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

继续解压，发现是有密码的，但是题目没有给任何提示，我们无法确定这个密码的长短，如果直接使用暴力破解的话肯定要花费很长的时间，所以暴力破解的思路肯定不对

那我们就继续在图片上找找，说不定会有密码

我们用老思路用StegSolve打开图片查看也没有找到任何信息，那我们就查查这个文件的EXIF

果然，在文件的属性中找到这么一句话

属性	值
说明	
标题	
主题	
分级	☆☆☆☆☆
标记	
备注	this_is_not_password
来源	
作者	
拍摄日期	
程序名称	
获取日期	
版权	
图像	
图像 ID	
分辨率	1366 x 768
宽度	1366 像素
高度	768 像素
水平分辨率	96 dpi
垂直分辨率	96 dpi
位深度	24
压缩	

这里就很值得怀疑，我们拿去试试是不是密码，结果这还真的就是压缩文件的密码

就得到了flag

## 第二十题 easycap

下载好附件后发现可以用wireshark打开，打开之后，我们用之前的思路去查询分组字节流中的flag，显示查不到

那就直接追踪数据包的TCP流，结果答案就这么明显的摆在眼前

```
FLAG:385b87afc8671dee07550290d16a8071
```

## 第二十一题 另外一个世界

打开附件发现是一个.jpg文件，继续用二进制编辑器打开仔细寻找发现里面有两个FF D8 FF，所以有两个.jpg文件，我们将这两个文件进行分离发现什么信息都没有，相反在源文件的基础上，我们直接搜索flag（66 6C 61 67）反而很轻易的看到了flag

```
2A 2A 2A 2A 2A 2A 2A 2A 2A 2A 0D 0A 66 6C 61 67 *****..fl ag
3A 62 61 73 65 36 34 3A 28 4D 7A 63 33 59 32 4A :base64:(Nzc3Y2J
68 5A 47 52 68 4D 57 56 6A 59 54 4A 6D 4D 6D 59 hZGRhNWVj YTJ nMmY
33 4D 32 51 7A 4E 6A 49 33 4E 7A 63 34 4D 57 59 3NzQzNj I 3Nzc4MmY
77 4D 47 45 3D 29 0D 0A 2A 2A 2A 2A 2A 2A 2A 2A wME=>.. *****
```

很明显这是用base64加密的，我们只需要去在线解密一下就ok

请输入要进行 Base64 编码或解码的字符

Mzc3Y2JhZGRhMWVjYTJmMmY3M2QzNjl3Nzc4MmYwMGE=

编码 (Encode)

解码 (Decode)

↑ 交换

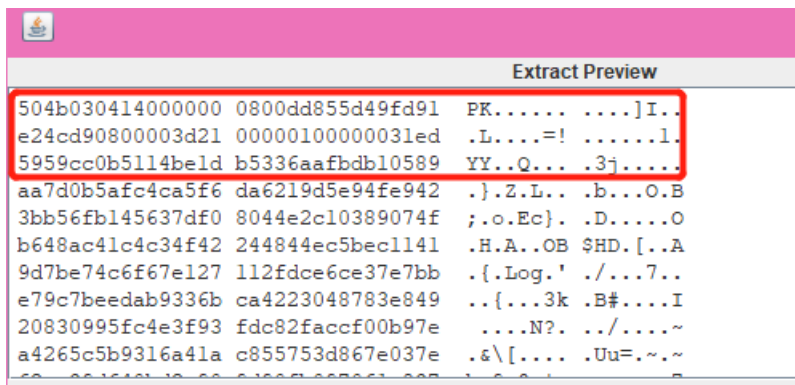
(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

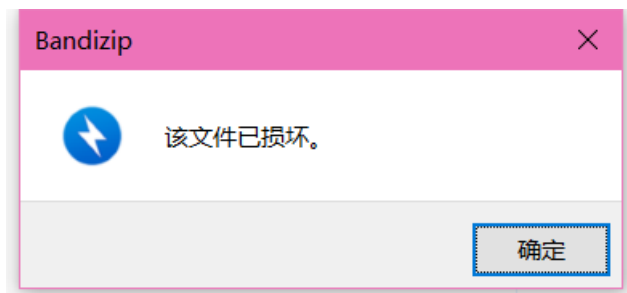
377cbadda1eca2f2f73d36277781f00a

## 第二十二题 FLAG

下载好附件之后发现是一个很很很搞笑的照片，我们还用之前的思路，拿二进制打开的话是一点信息都没有的，是一个很纯很纯的.png文件，所以我们猜测可能是用了LSB隐写，我们拿StegSolve打开它，分析它的数据



发现这里应该是隐藏了.zip文件，我们将它分离出来，命名成.zip文件，打开的话提示我们数据损坏



这里可以不用管它，继续打开里面的文件就好

打开发现是一堆乱码，但是我们在乱码中找到了最重要的东西



]?F□ □□□@ H7□ t? H?H?U?□ H? 取? □ □ UH?控□@? ? 枕? ]?□? □@ AWA?AVI?AUI?ATL?? UH?? SL)?? 第□H?□? H?□? L?L?D?A □□□□H9?□□[A]A^A ?f□? □ H?□H?□? □ hctf(dd0gf4c3tok3yb0ard4g41n~~~) □□□0

题目上提示了把hctf换成flag就好

## 第二十三题 假如给我三天光明

呼~

这应该是目前遇到最难的一道题了

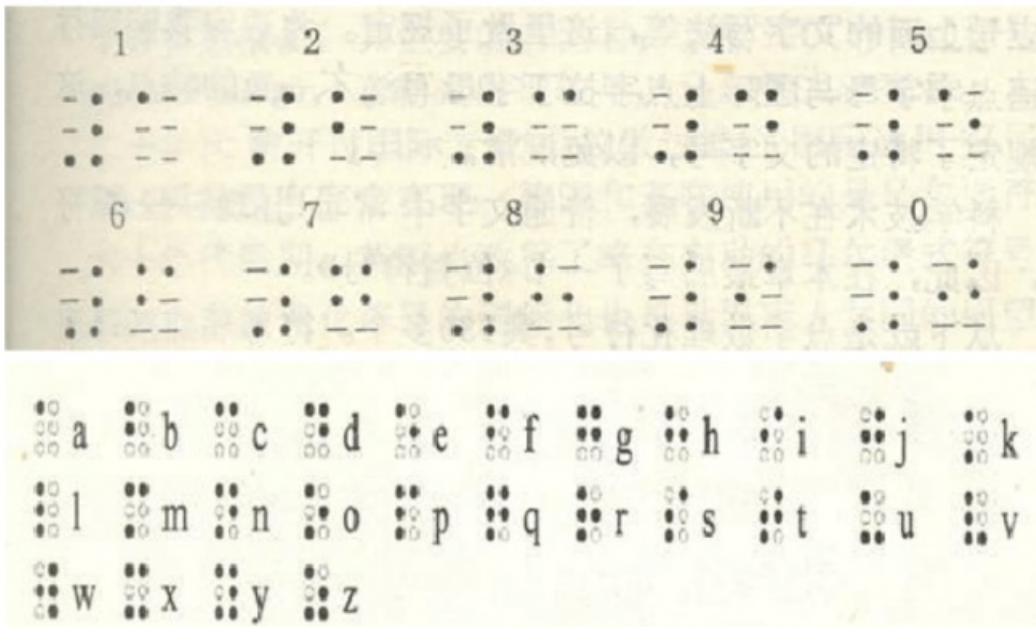
打开附件后发现，有一个照片和被加密的压缩包，那么密码肯定在这个照片里

打开发现照片底下的确藏有东西，但是不知道是什么



首先猜测的是二进制，但是按它两位两位排列只能写三个数字，所能隐藏的信息太少了，所以应该不是二进制

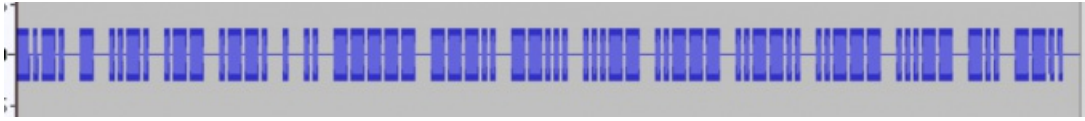
题目给了我们很大的提示“假如给我三天光明”，这该不是盲文吧，百度一下，嘿！盲文还真的就长这个样子



然后就推出密码是 **kmdonowg**

打开压缩包发现是个音频文件，听的话是摩斯密码，但是我实在太菜了，靠听真的听不出来，所以只能借助工具——Audacity

我们获得这个.wav的波形图



长的一段是-,短的一段是.,然后结合摩斯密码表就得到了答案

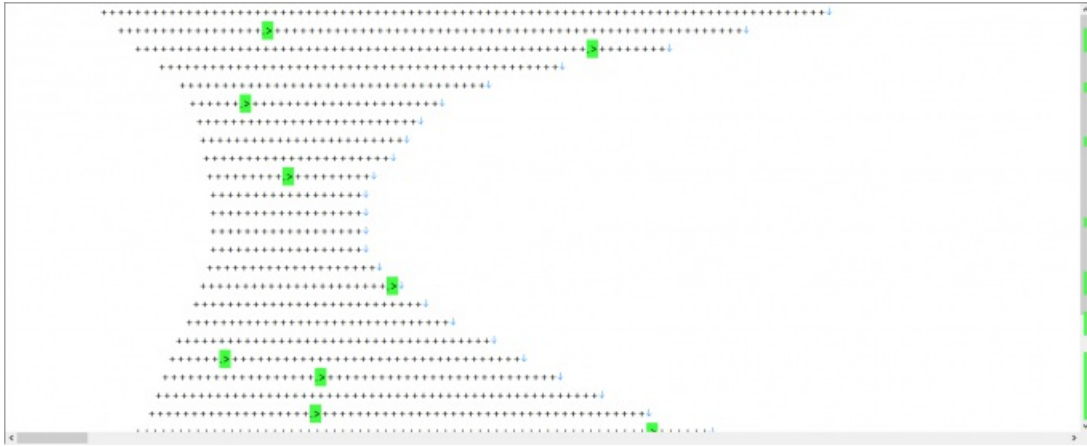
1	- . - .	c
2	-	t
3	. . - .	f
4	. - -	w
5	. - - .	p
6	.	e
7	. .	i
8	- - - - -	0
9	- - - . .	8
▶10	- - . . .	7
11	. . . - -	3
12	. . - - -	2
13	. . - - . .	?
14	. . - - -	2
15	. . . - -	3
16	- . .	d
17	- - . .	z

## 第二十四题 神秘的龙卷风

根据题目知道，这个压缩包的是由四位密码组成的，我们用爆破工具爆破

日志窗口	
开始时间	状态与结果
2021-5-28 16:16:26	开始恢复文件的密码:神秘龙卷风.rar
2021-5-28 16:16:53	恢复成功,密码是:5463

打开压缩包发现是一个.txt文档，可是打开后发现真的是外星人语言



这下可真的啥也不知道了，只能百度搜题解，发现这是一种编程语言叫brainfuck

可以在线执行 (<http://bf.doleczek.pl/>)

```
flag{e4bbef8bdf9743f8bf5b727a9f6332a8}y
```

## 第二十五题 后门查杀

这是一道看起来很难很难的题，它有一大堆的.php文件

题目上提示是webshell上传，我们直接用杀软扫描刚刚下载好的附件，如果真的存在webshell上传的话，那么一定会报毒的



我们按照路径找到那个文件

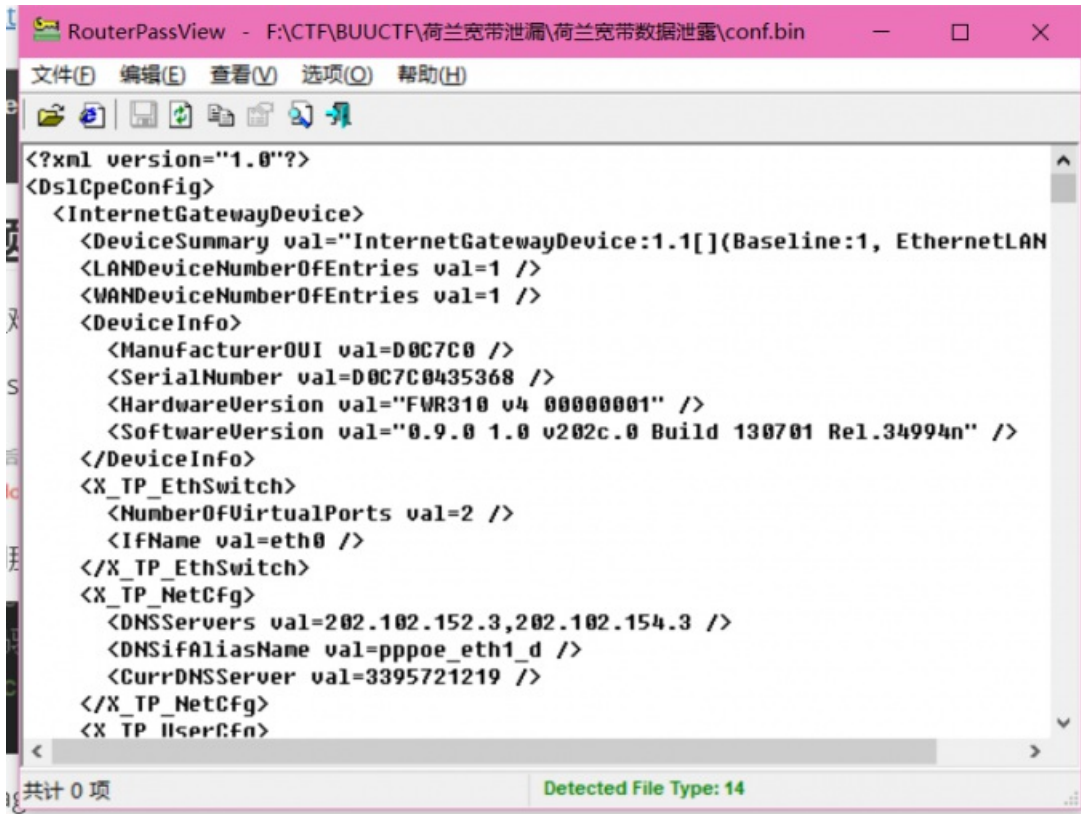
```
//如果需要密码验证,请修改登陆密码,留空为不需要验证  
$pass = '6ac45fb83b3bc355c024f5034b947dd3'; //angel
```

很容易就能找到flag

## 第二十六题 荷兰宽带数据泄漏

根据题目信息得到这是文件应该是宽带数据流量，那么我们就需要用相对应得工具打开，百度到的是需要用routerpassview打开

那就下个它打开文件



按照我们之前做题的经验，flag一般会藏在用户名或者密码当中，我们就在这堆数据里找username和password，然后一个一个去提交，看那个是真正的flag

终于我们找到了那个万恶的flag

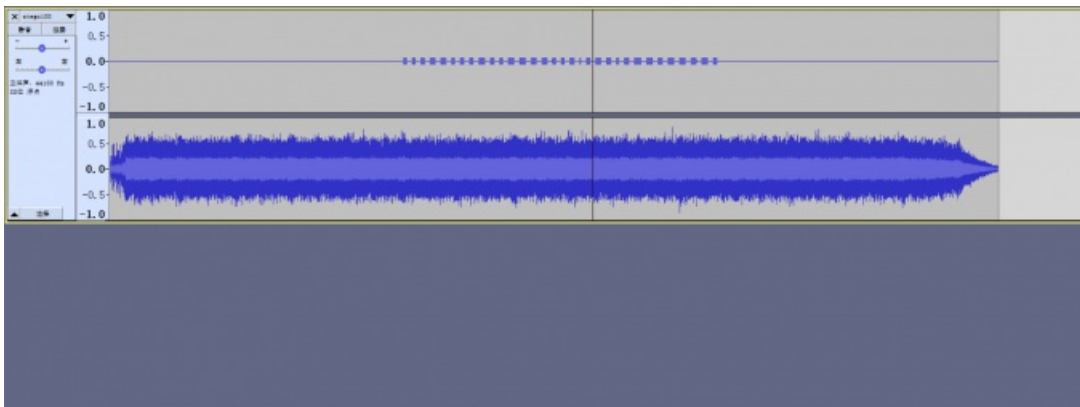
```
<Username val=053700357621 />  
<Password val=210265 />
```

就是用户名

## 第二十七题 来首歌吧

打开附件之后发现是一个音频文件

我们还用Audacity进行查看，发现在这首歌中有两个轨道



而上面那一条轨道正是莫斯密码

我们将其写下来

.....

再在线转换一下就得到了flag

英文字母:  
5BC925649CB0188F52E617D70929191C



转换为摩斯电码 清除 生成摩斯代码的分隔方式:  空格分隔  单斜杠/分隔

摩斯电码: (格式要求: 可用空格或单斜杠/来分隔摩斯电码, 但只可用一种, 不可混用)

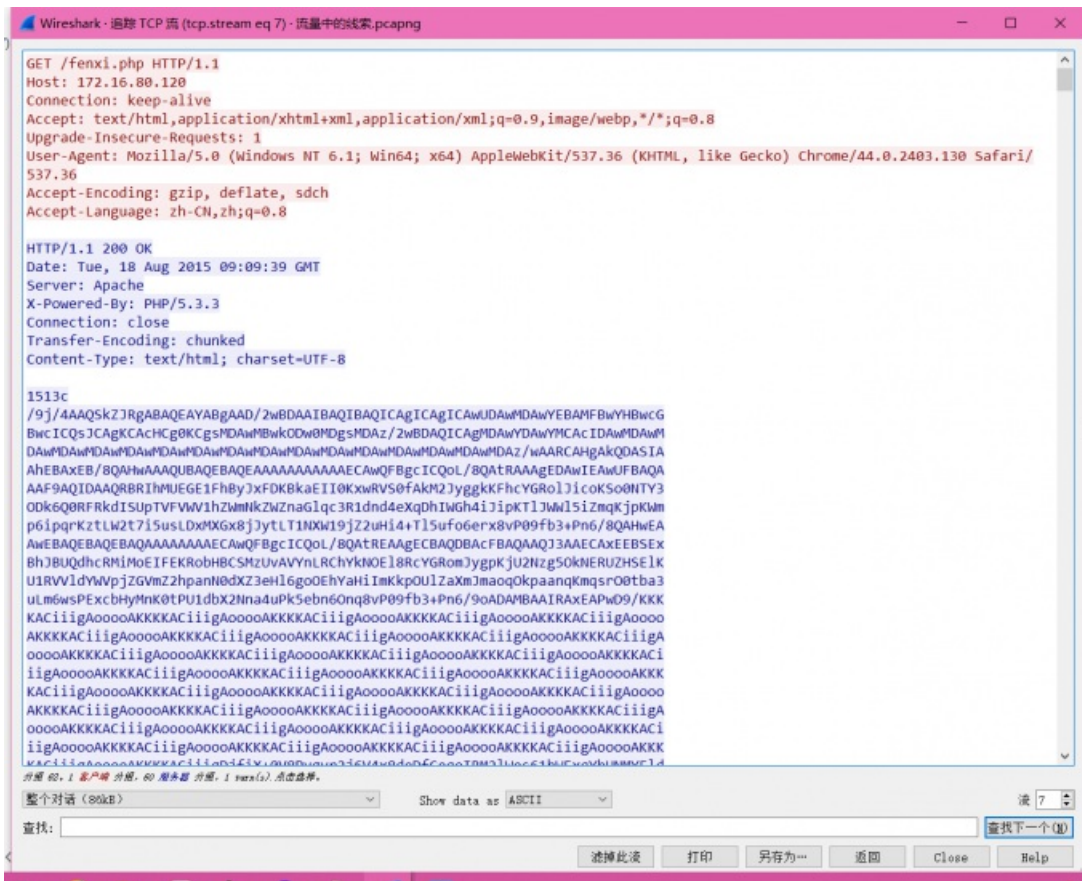
.....

## 第二十八题 数据包中的线索

下载好附件后用wireshark打开, 我们可以一个一个分析这些数据包, 发现只有一种类型的数据包是很可疑的, 它与其他数据包很不一样, 其他数据包没有多少信息, 而只有这个数据包里含有很多信息

0000	0c da 41 9e cc 85 20 89 84 32 73 c5 08 00 45 00	..A... .2s...E.
0010	01 a9 45 dc 40 00 40 06 00 00 ac 10 42 64 ac 10	..E.@.@. ....Bd..
0020	50 78 07 5b 00 50 c1 88 86 87 21 e5 02 ac 50 18	Px.[.P... !...P.
0030	40 29 ec 98 00 00 47 45 54 20 2f 66 65 6e 78 69	@)....GE T /fenxi
0040	2e 70 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a 48	.php HTTP/1.1..H
0050	6f 73 74 3a 20 31 37 32 2e 31 36 2e 38 30 2e 31	ost: 172 .16.80.1
0060	32 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20	20..Conn ection:
0070	6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 63 63 65	keep-ali ve..Acce
0080	70 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70	pt: text /html,ap
0090	70 6c 60 63 61 74 60 6f 60 2f 70 60 74 6d 6c 2b	lication/html.

我们进行追踪它的TCP流



这里看起来就很可疑了，貌似是base64编码，我们在一个网站进行在线解码一下（<https://the-x.cn/base64>）



发现是一个.jpg文件，我们下载打开，就发现了神奇的小秘密

flag{209acebf6324a09671abc31c869de72c}



## 第二十九题 九连环

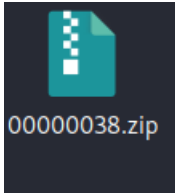
我们下载好附件后发现是一个.jpg文件，按照之前的旧思路用二进制编辑器打开，我们去搜索.zip的文件头（50 4B 03 04）发现有很多，而且根据题目“九连环”也感觉这个文件不是那么简单

```
10 84 02 10 84 07 FF D9 50 4E 03 04 0A 00 00 08
00 00 AE 54 53 4B 00 00 00 00 00 00 00 00 00
00 00 04 00 00 00 61 73 64 2F 50 4E 03 04 14 00
```

我们就打开kali用binwalk分析一下

```
root@kali2020:~/桌面# binwalk 123456cry.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
19560       0x4C68      Zip archive data, at least v1.0 to extract, name: asd/
48454       0xBD46      Zip archive data, at least v1.0 to extract, compressed size: 184, uncompressed size: 184, name: asd/qwe.zip
48657       0xBE11      End of Zip archive, footer length: 22
48962       0xBF42      End of Zip archive, footer length: 22
```

发现果然有东西，那就用foremost分离一下



得到了一个.zip文件

打开的话发现是有密码的，那就不用二进制编辑器判断一下是不是伪加密

```
31 83 48 D3 01 50 4E 01 02 3F 00 14 00 01 08 08 1. H. PK. ?. . . . .
00 48 4E 53 4B 8C 3A D5 7E 88 70 00 00 28 75 00 . H&K :. ~. p. (u
```

果然是伪加密，将01 08修改成00 08，绕过伪加密



good-已合并.jpg



qwe.zip

发现里面只有一个.jpg和一个加密了的压缩包

而照片里没有提供任何信息（用之前解密.jpg的思路）

这里用steghide来破解

```
root@kali2020:~/桌面# steghide extract -sf good-已合并.jpg
Enter passphrase:
wrote extracted data to "ko.txt".
```

- 1 看到这个图片就是压缩包的密码：
- 2 bV1g6t5wZDJif^J7

输入密码解压之后就能看到flag了

### 第三十题 面具下的flag

打开附件发现是一个.jpg照片，用二进制编辑器打开的话可以搜索到文件中包含50 4B 03 04，可以断定文件中隐藏了.zip文件

用binwalk分析一下





## 第三十一题 webshell后门

详细解法请参考第第二十五题