




BUUCTF misc 解题记录 一（超级详细）

原创

[Vayn3](#)  于 2021-03-16 23:37:03 发布  3030  收藏 36

分类专栏: [笔记](#) 文章标签: [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/qq_51090016/article/details/114906829

版权



[笔记](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

持续更新一些不会的题目, 有错误的还请大佬指点

N种方法解决(运行不了的文件尝试改成txt文件)

LSB (图片通道上方隐藏信息用save bin)

zip伪加密

另外一个世界 (二进制转字符: ASCII码)

FLAG (save bin 分析文件类型)

假如给我三天光明 (盲文)

后门查杀 (用d盾查杀木马)

面具下的flag(用7z解压缩vmdk文件)

九连环 (steghide)

snake (serpent解密)

菜刀666 (流量分析)

[SWPU2019]神奇的二维码 (binwalk -e分离)

[ACTF新生赛2020]outguess (outguess的用法)

谁赢了比赛?

[HBNIS2018]excel破解 (修改后缀)

喵喵喵 (奇怪的lsb NTFS文件流隐写)

[HBNIS2018]来题中等的吧 (条形码表示摩斯电码)

弱口令 (这也能藏莫斯代码? 没遇到过的lsb隐写)

[SWPU2019]你有没有好好看网课? (敲击码)

john-in-the-middle(导出http)

低个头 (键盘加密??)

zip

我吃三明治(两张图拼接之间隐藏信息)

间谍启示录 (奇怪的题目)

[SUCTF2018]single dog(AAEncode解密)

[安淘杯 2019]吹着贝斯扫二维码

从娃娃抓起 (中文电码)

小易的U盘 (ida的使用)

[ACTF新生赛2020]swp (导出http)

百里挑一

[WUSTCTF2020]alison_likes_jojo (outguess隐写)

[GUET-CTF2019]zips (伪加密 python时间戳?)

[安淘杯 2019]Attack (mimikatz的使用)

[SUCTF 2019]Game

[WUSTCTF2020]girlfriend (DTMF拨号音 手机键盘密码)

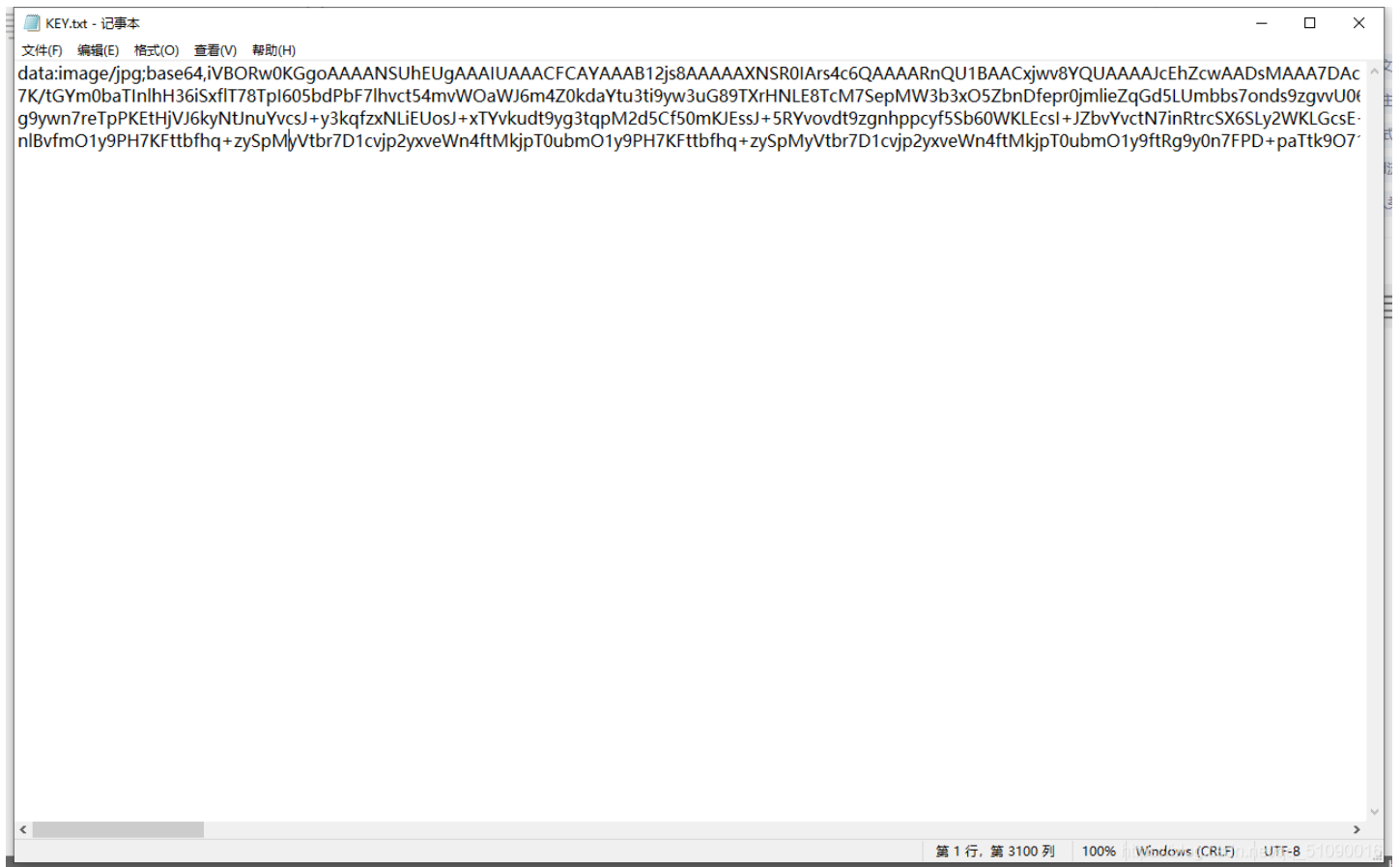
[MRCTF2020]CyberPunk

USB (USB数据包 维吉尼亚解密)

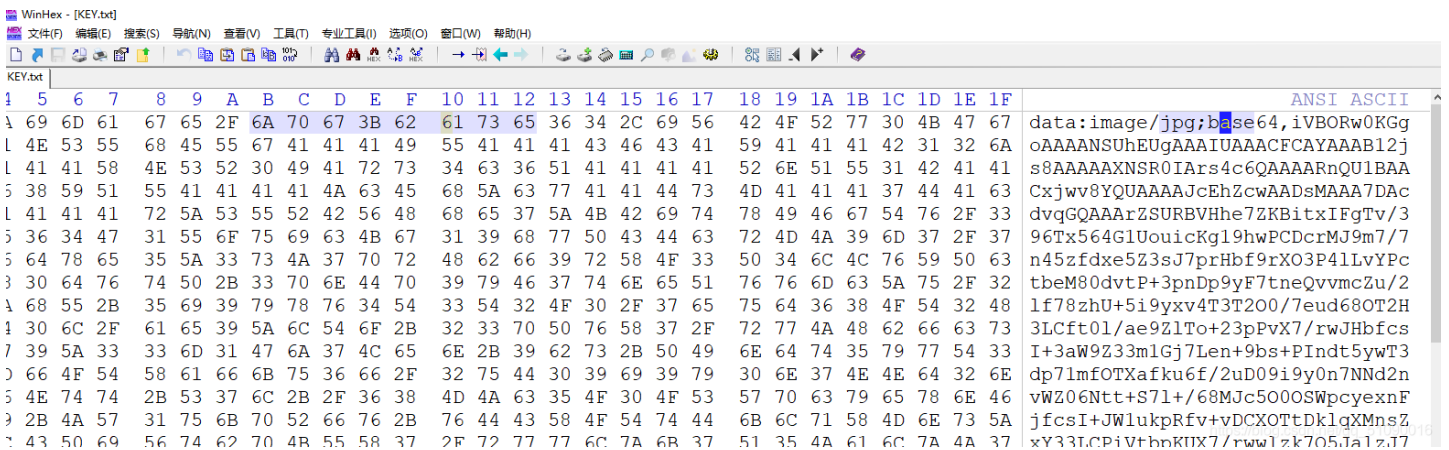
N种方法解决(运行不了的文件尝试改成txt文件)

附件下载是一个exe文件, 我还运行不了。。这咋办

改成txt文件看看



好像有什么东西藏在里面 前面有个jpg 还有base，用winhex打开看看



到这没思路了，看wp

base64可以表示图片

这个让我这个菜鸡人傻了

[转换网站点这](#)

转换完还能帮你另存为，真不错

Base64 仕线解码、编码

常规Base64

CSS Base64

DES加密/解密

3DES加密/解密

AES加密/解密

RSA加密/解密



点击关闭

```
WR/e0faJ7Xdzw/bMKbGc7PbNE1x3uqNtn9h+Nzdsz5wSy8lu3zzBdac72vaJ7Xdzw/bMKbGc7PbNE1x3uqNtn9h+Nzdsz5wSy8lu3zzBcsVewpyS1LmTWG
7Y3nLCPm1JN05KLP/D8tRGzCjInTuJ5YbtLSfs05Z046TE8j8sT23EnJLUuZNYbtjecsI+bUk3Tkos/8Py1EbMKUmdO4nlhu0tJ+zTlnTjpMTyP/Ri8Pwl//fJZ
Yb3Jvv8Pd/ll+WWG5wb77D3/8pfllicG9+Q5//6f4ZYnlBvfmO1y9PH7KfTtbhq+zySpMyVtr7D1cvjp2yxveWn4ftMkjpT0ubmO1y9PH7KfTtbhq+zySpMyVt
br7D1cvjp2yxveWn4ftMkjpT0ubmO1y9ftRg9y0n7FPD+paTtk9O71sT13Mv7WD3LSfsU8P6lpO2T07VWxPXcy/tYPctJ+xTw/qWk7ZPTu9bE9dzL+1g9y0n7
FPD+paTtk9O71sT1/P7EnOTWG5wb5LumRptn3
ZPuP90X9+8PpwwN0mb72pYfzcn1rf8NHwffXXV
OuvDCXOT7OZGu7e+5YT9XynlhH36DlVfsTcLL
+1GD3LX8avt8Klhu2t5yc6F+/68OT2H3Ln4bvN4n
7K05y+z3smsbyF93Z9h6uXx095mtP3ec8krfw3q
```

```
D4 46 CC 29 49 9D 3B 89 E5 86 ED 2D
74 E3 A4 C4 F2 3F 2C 4F 6D C4 9C 92
6E D8 DE 72 C2 3E 6D 49 37 4E 4A 2C
46 CC 29 49 9D 3B 89 E5 86 ED 2D 27
E3 A4 C4 F2 3F F4 7F 8B C3 F0 23 FF DF 25 96 1B
DC 9B EF F0 F7 7F 8A 5F 96 58 6E 70 6F BE C3 DF
FF 29 7E 59 62 B9 C1 BD F9 0E 7F FF A7 F8 65 89
E5 06 F7 E6 3B 5C BD 3C 7E CA 16 DB 5B 7E 1A BE
CF 24 A9 33 25 6D 6E BE C3 D5 CB E3 A7 6C B1 BD
E5 A7 E1 FB 4C 92 3A 53 D2 E6 E6 3B 5C BD 3C 7E
CA 16 DB 5B 7E 1A BE CF 24 A9 33 25 6D 6E BE C3
D5 CB E3 A7 6C B1 BD E5 A7 E1 FB 4C 92 3A 53 D2
E6 E6 3B 5C BD 7E D4 60 F7 2D 27 EC 53 C3 FA 96
93 B6 4F 4E EF 5B 13 D7 73 2F ED 60 F7 2D 27 EC
53 C3 FA 96 93 B6 4F 4E EF 5B 13 D7 73 2F ED 60
F7 2D 27 EC 53 C3 FA 96 93 B6 4F 4E EF 5B 13 D7
73 2F ED 60 F7 2D 27 EC 53 C3 FA 96 93 B6 4F 4E
EF 5B 13 D7 F3 FB 12 73 93 58 6E 70 6F 92 D4 99
1A 6D 9F 70 FF E9 BE BE 79 7D 38 61 6E 12 CB 0D
EE 4D 92 3A 53 A3 ED 13 EE 3F DD D7 37 AF 0F 27
```

新建下载任务

文件名: from_base64@the-x (1).png

保存到: 你没办法\Pictures\CSDN博客\buu

中文编码: UTF-8

插件【Png】Png Image

附加信息:

Size:133x133

另存为: png文件

当前编码: [Hex]

数据长度: 2884 Bytes

插件数: 16, 耗时: 0ms



https://blog.csdn.net/qq_51090016

https://blog.csdn.net/qq_51090016

扫一下就OK了

from_base64@the-x.png



KEY{dca57f966e4e4e31fd5b15417da63269}

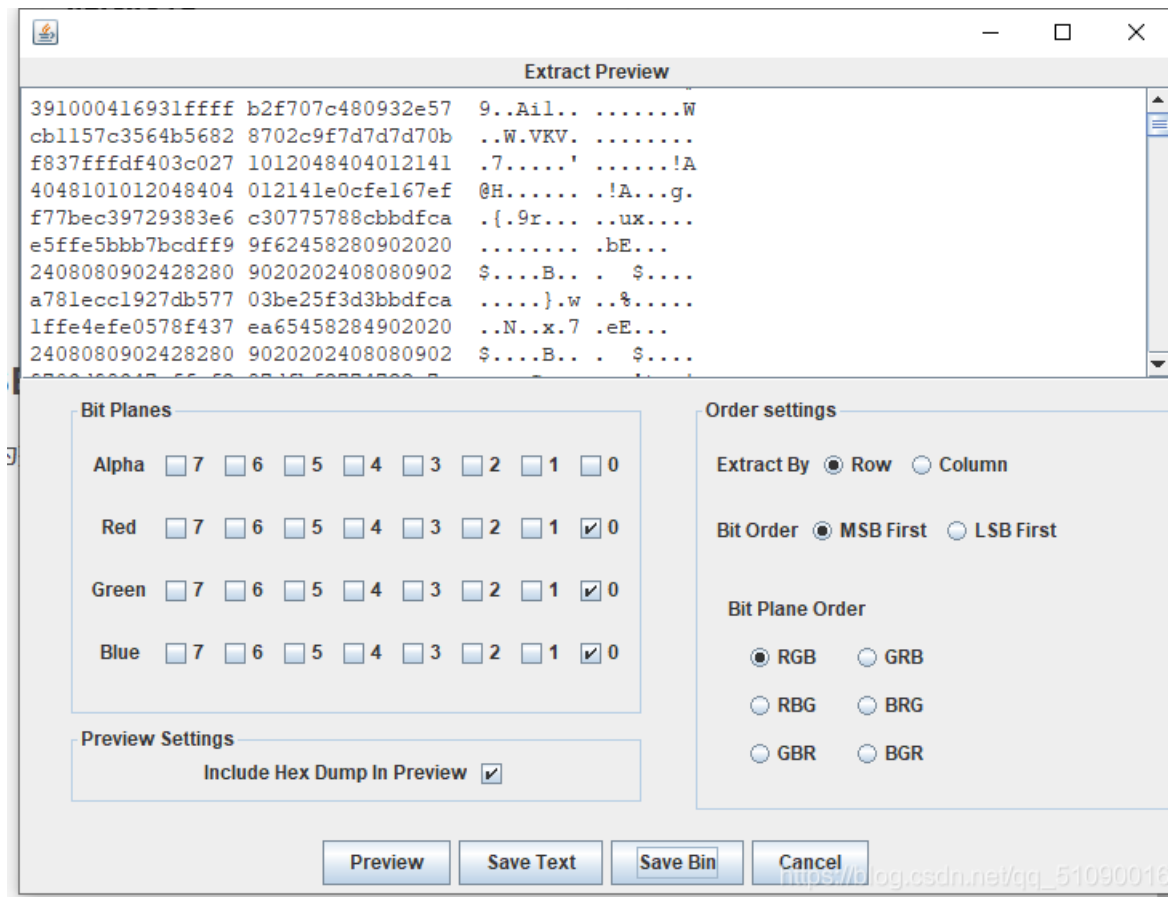
扫描识别

https://blog.csdn.net/qq_51090016

LSB (图片通道上方隐藏信息用save bin)

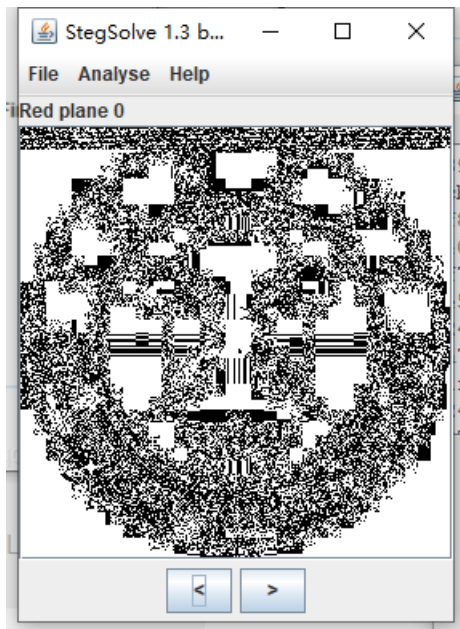
因为提示lsb, 所以先用stegsolve打开看看

这样设置就行了



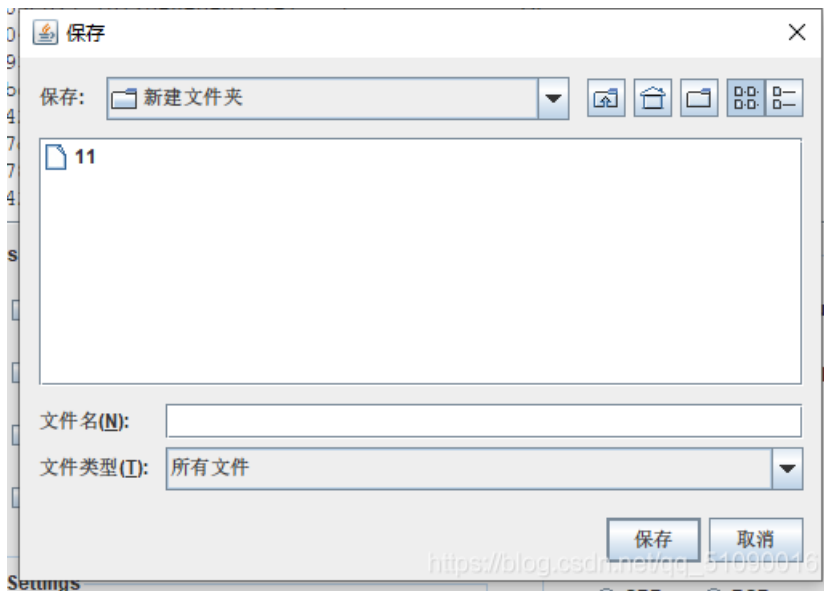
开始我以为这就完事了, 傻傻的把{}里面的当成flag了

输了发现不是, 然后又更换了几个选项, 还是不行, 只好看看wp

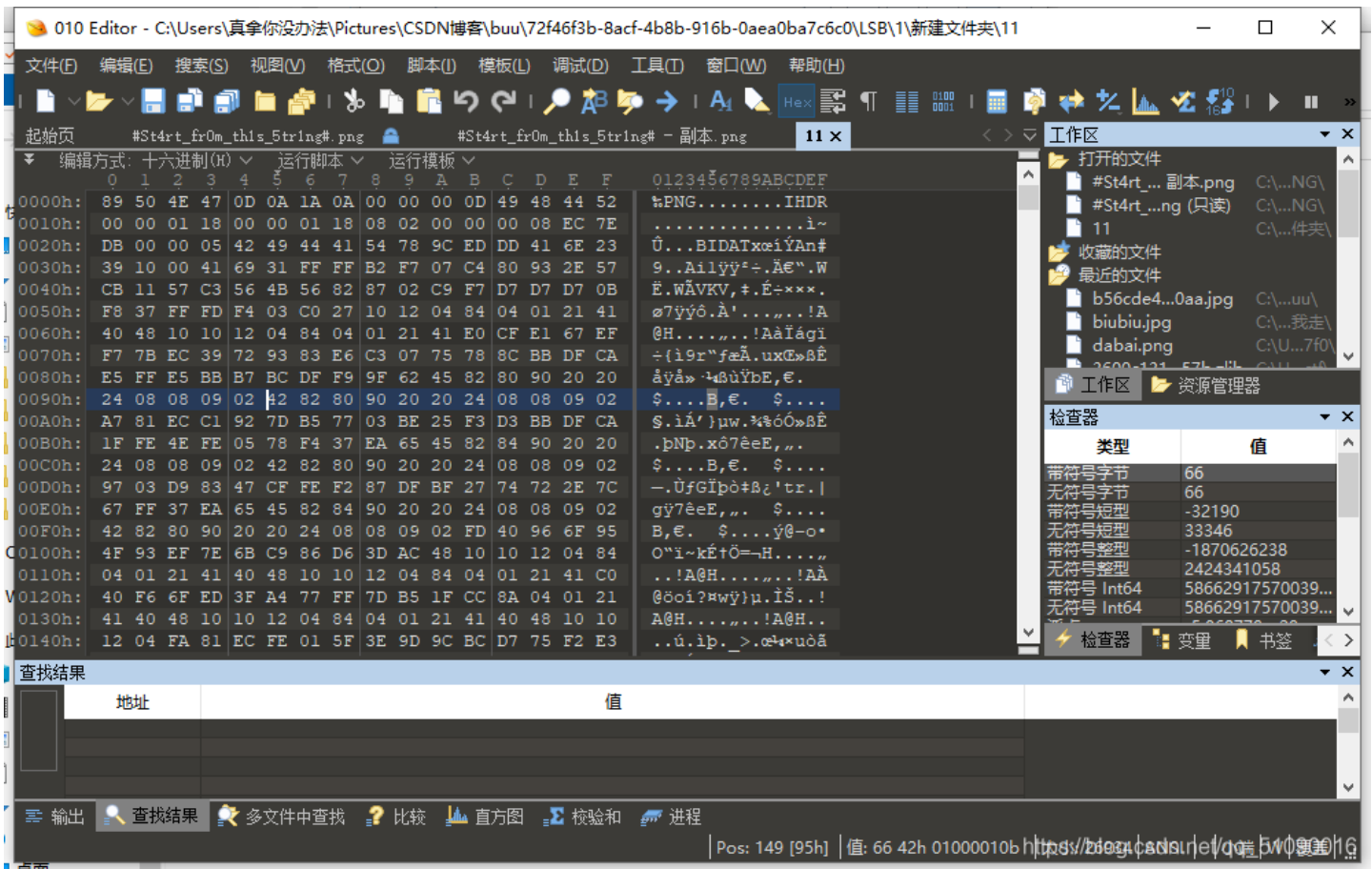


原来要查看图片通道:

发现这上面好像隐藏着东西, 这样就要用到save bin的操作



保存后用哦010打开看看



发现是png文件

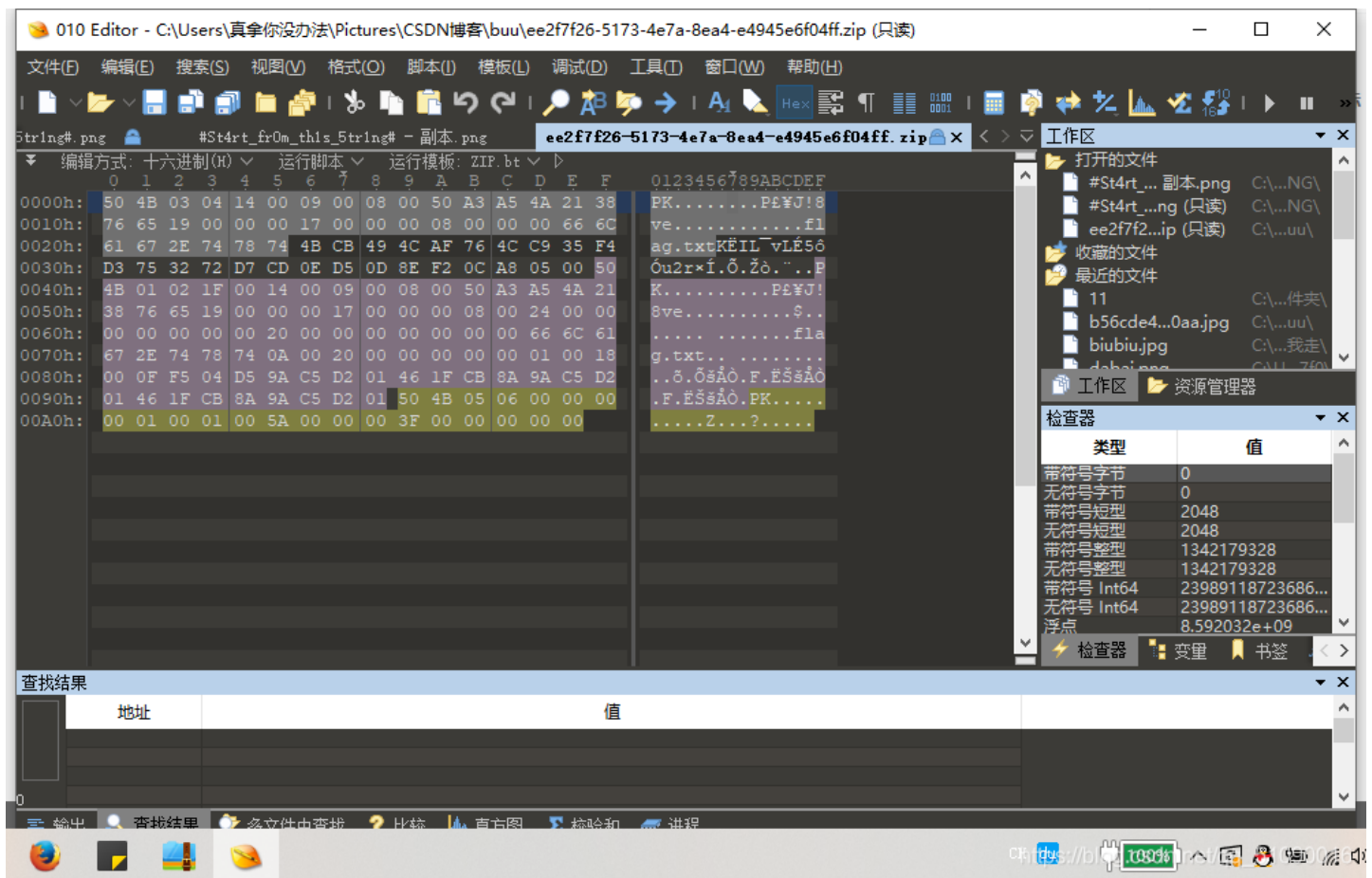


这样就有了

zip伪加密

刚好借着这题把我没搞懂的伪加密弄懂

首先肯定是用010打开



我记得伪加密应该是把什么09改成00吧，既然不记得了，来系统的学习一下，转载大佬的博客

来了解一下ZIP文件的组成

一个 ZIP 文件由三个部分组成：

压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

a.压缩源文件数据区：

50 4B 03 04：这是头文件标记（0x04034b50）

14 00：解压文件所需 pkware 版本

00 00：全局方式位标记（有无加密，奇数加密，偶数无加密）

08 00：压缩方式

5A 7E：最后修改文件时间

F7 46：最后修改文件日期

16 B5 80 14：CRC-32校验（1480B516）

19 00 00 00：压缩后尺寸（25）

17 00 00 00：未压缩尺寸（23）

07 00：文件名长度

00 00：扩展记录长度

6B65792E7478740BCECC750E71ABCE48CDC9C95728CECC2DC849AD284DAD0500

b.压缩源文件目录区：

1

50 4B 01 02：目录中文件文件头标记(0x02014b50)

3F 00：压缩使用的 pkware 版本

14 00：解压文件所需 pkware 版本

00 00：全局方式位标记（有无加密，奇数加密，偶数无加密）

08 00：压缩方式

5A 7E：最后修改文件时间

F7 46：最后修改文件日期

16 B5 80 14：CRC-32校验（1480B516）

19 00 00 00：压缩后尺寸（25）

17 00 00 00：未压缩尺寸（23）

07 00：文件名长度

24 00：扩展字段长度

00 00：文件注释长度

00 00：磁盘开始号

00 00：内部文件属性

20 00 00 00：外部文件属性

00 00 00 00：局部头部偏移量

6B65792E7478740A0020000000000010018006558F04A1CC5D001BDEBDD3B1CC5D001BDEBDD3B1CC5D001

c.压缩源文件目录结束标志：

1

50 4B 05 06：目录结束标记

00 00：当前磁盘编号

00 00：目录区开始磁盘编号

01 00：本磁盘上纪录总数

01 00：目录区中纪录总数

59 00 00 00：目录区尺寸大小

3E 00 00 00：目录区对第一张磁盘的偏移量

00 00 1A：ZIP 文件注释长度

版权声明：本文为CSDN博主「宁嘉」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

这么一串二进制肯定有问题，我开始的想法是转成16进制再转字符

什么是JSON JSON的用法 华为云开年采购季 腾讯云双12(88元/年) 恒

16进制到文本字符串

加密或解密字符串长度不可以超过10M

1	6b6f656b6a3374
---	----------------

16进制转字符 字符转16进制 测试用例 清空结果 复制结果

互动直播SDK

30分钟集成ZEGO SDK，轻松实现语音互动直播和视频互动直播，让直播科技

1	koekj3t
---	---------

https://blog.csdn.net/qq_51090016

得到这个

然后一直不对，看wp，答案是这个

koekj3s|

wp是将每八位二进制数字分开，用ASCII码得到的

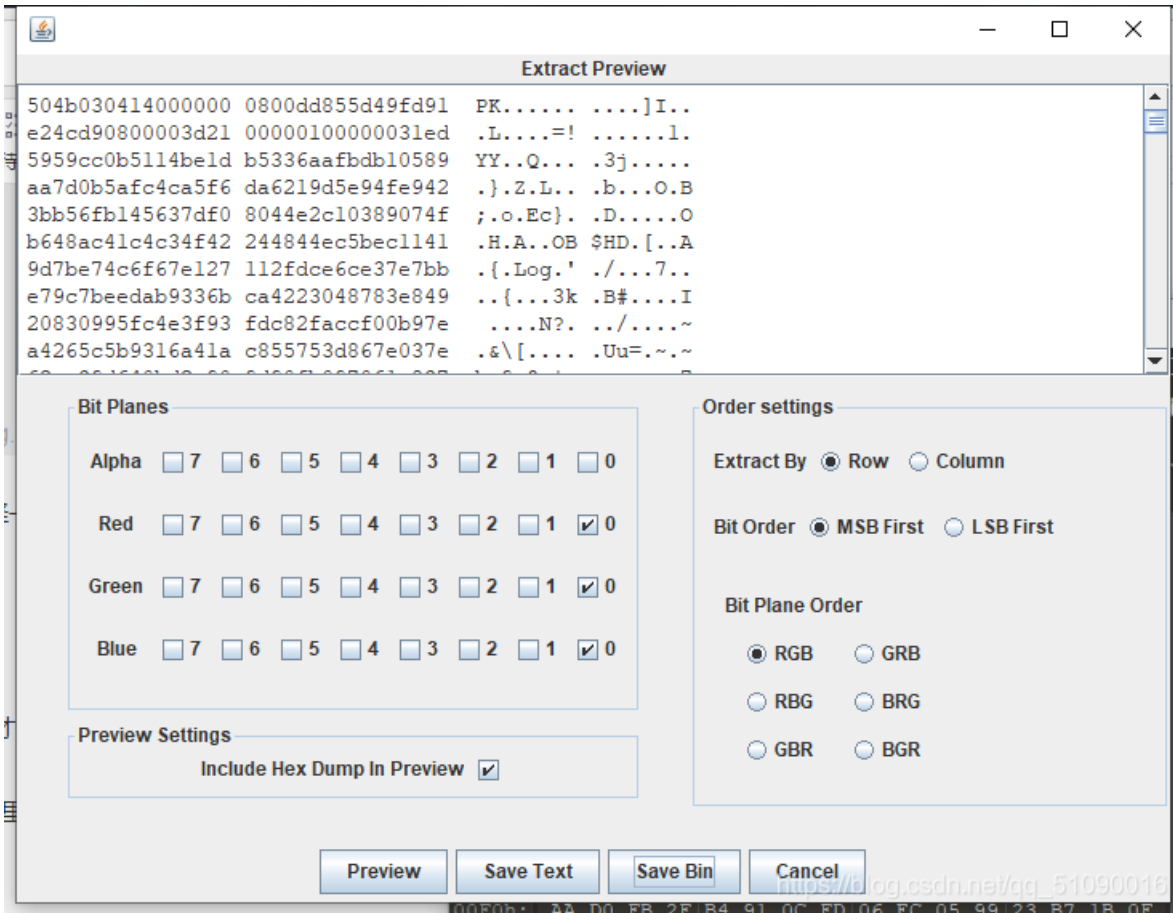
```
01101011
01101111
01100101
01101011
01101010
00110011
01110011
```

为什么就差一个字母不一样？不懂，有大佬解释一下嘛

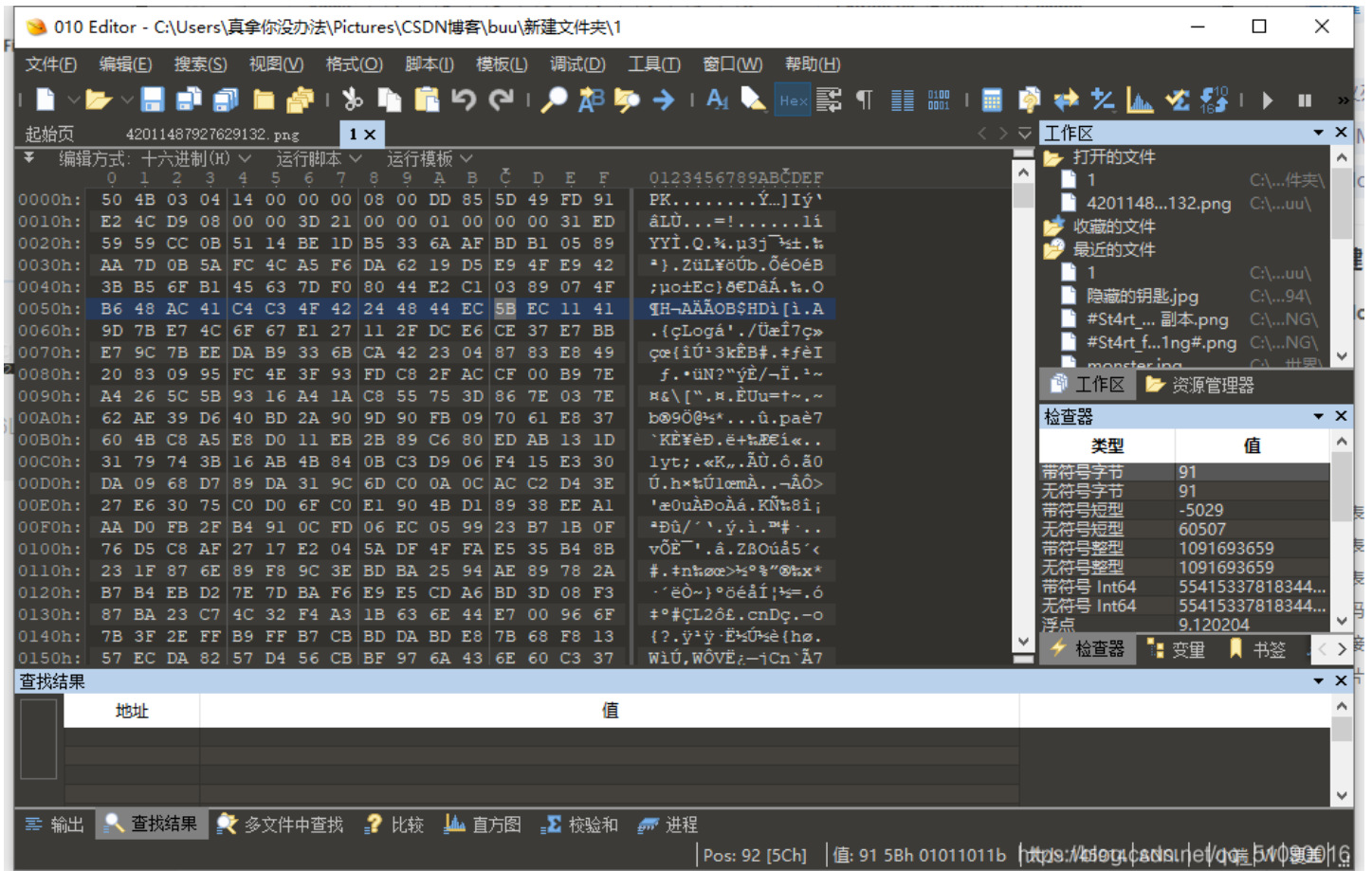
FLAG (save bin 分析文件类型)

这题是因为写了一半卡住了没思路。。看了wp才知道可惜了

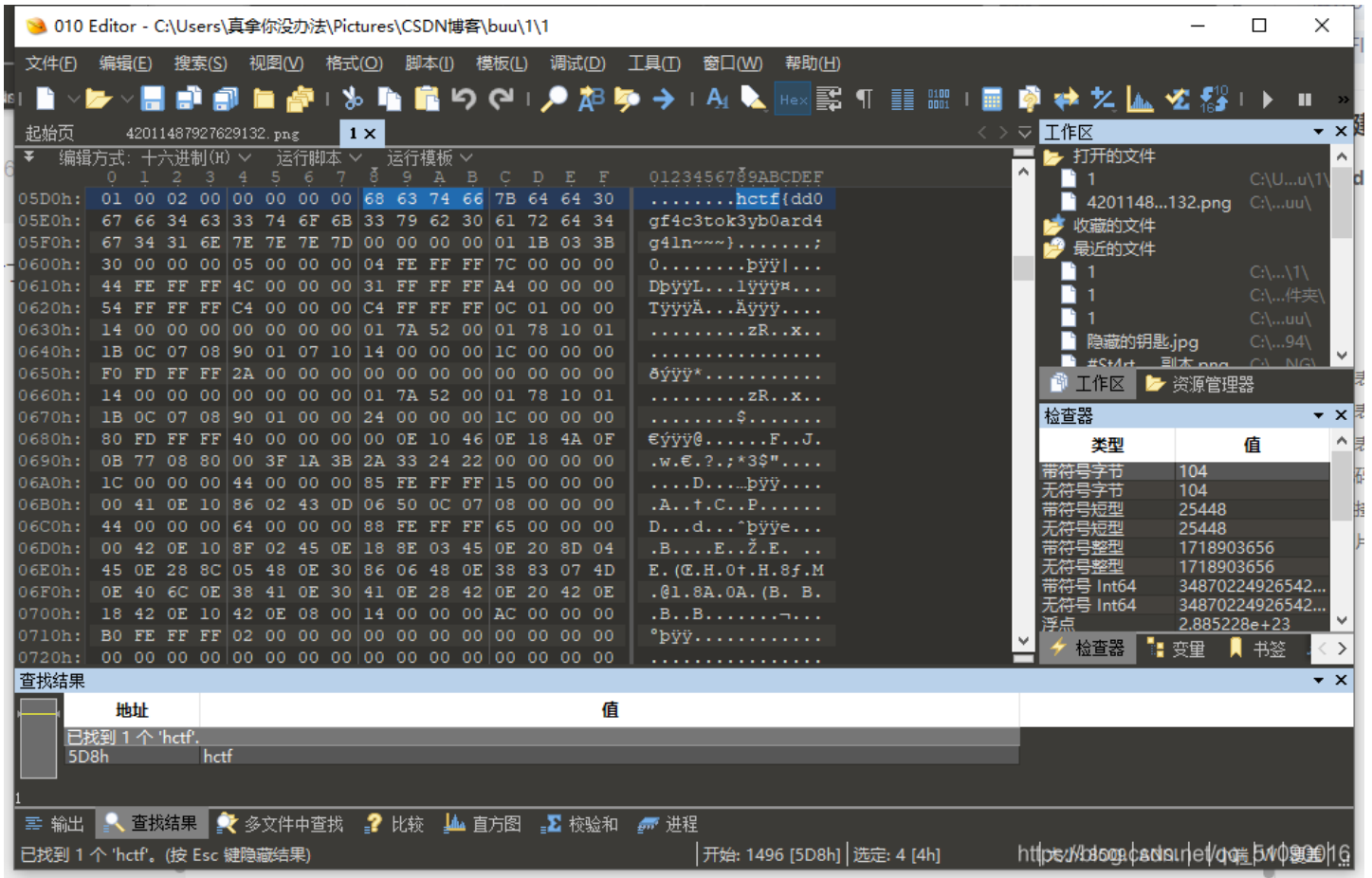
其他方法都试过了，010打开看的时候也没发现里面藏了文件，所以最后用stegsolve打开看看是不是lsb



因为前面那题save bin的先例，所以这题我也试试，用010打开



但是我不知道这就是压缩包文件，所以就没做出来，后缀改成zip，解压后用010打开就有了

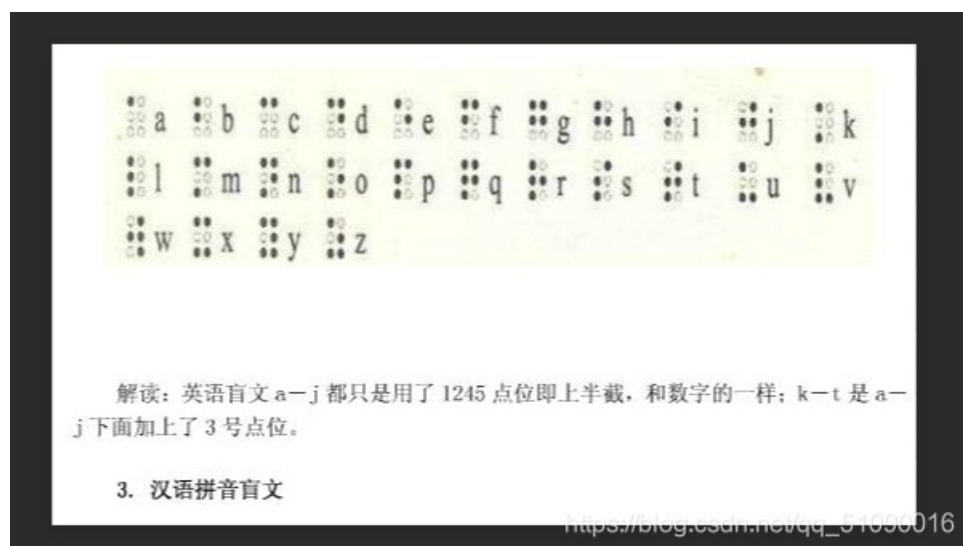


假如给我三天光明（盲文）

实在没想到下面这个是盲文（不应该）



搜盲文对照一下



也就是：kmdonwg

这样就能解压出音频文件了

差点以为点错地方了，还以为是web题呢

这里需要用到一个工具会比较简单：d盾

直接扫描大文件夹（文件太多了一个个看太麻烦）

The screenshot shows the D盾 v2.1.5.4 [测试版] interface. The main window displays the scan results for a directory. The interface includes a search bar, a navigation menu, and a table of scan results.

扫描结束. 检测文件数: 462 发现可疑文件: 3 用时: 0.52秒

文件 (支持拖放目录和扫描)	级别	说明	大小	修改时间
c:\users\真拿你没办法\pictures\csdn博客\buu...	1	phpinfo	22	2013-09-05 01:32:14
c:\users\真拿你没办法\pictures\csdn博客\buu...	3	可疑引用: [\$_GET[act]. ".php"]	41	2013-09-05 01:31:50
c:\users\真拿你没办法\pictures\csdn博客\buu...	5	多功能大马	58057	2015-07-09 17:08:21

Navigation: 主页 | 查杀 | 工具 | 规则 | 记录 | 选项

URL: https://blog.csdn.net/qq_51090016

webshell应该就是一句话木马吧，那查看一下下面的这个

```
include.php - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
if( strpos( strtolower( $_SERVER['HTTP_USER_AGENT'] ), 'bot' ) !== false ) {
    header('HTTP/1.0 404 Not Found');
    exit;
}
ob_start();
$mtime = explode(' ', microtime());
$starttime = $mtime[1] + $mtime[0];
define('SA_ROOT', str_replace('\\', '/', dirname(__FILE__)).'/');
define('SELF', $_SERVER['PHP_SELF'] ? $_SERVER['PHP_SELF'] : $_SERVER['SCRIPT_NAME']);
define('IS_WIN', DIRECTORY_SEPARATOR == '\\');
define('IS_GPC', get_magic_quotes_gpc());
$dis_func = get_cfg_var('disable_functions');
define('IS_PHPINFO', (!ereg("phpinfo",$dis_func) ? 1 : 0);

if( IS_GPC ) {
    $_POST = s_array($_POST);
}
$P = $_POST;
unset($_POST);
/*===== 程序配置 =====*/

//echo encode_pass('angel');exit;
// 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

//如您对 cookie 作用范围有特殊要求,或登录不正常,请修改下面变量,否则请保持默认
// cookie 前缀
$cookiepre = "";
// cookie 作用域
$cookiedomain = "";
// cookie 作用路径
```

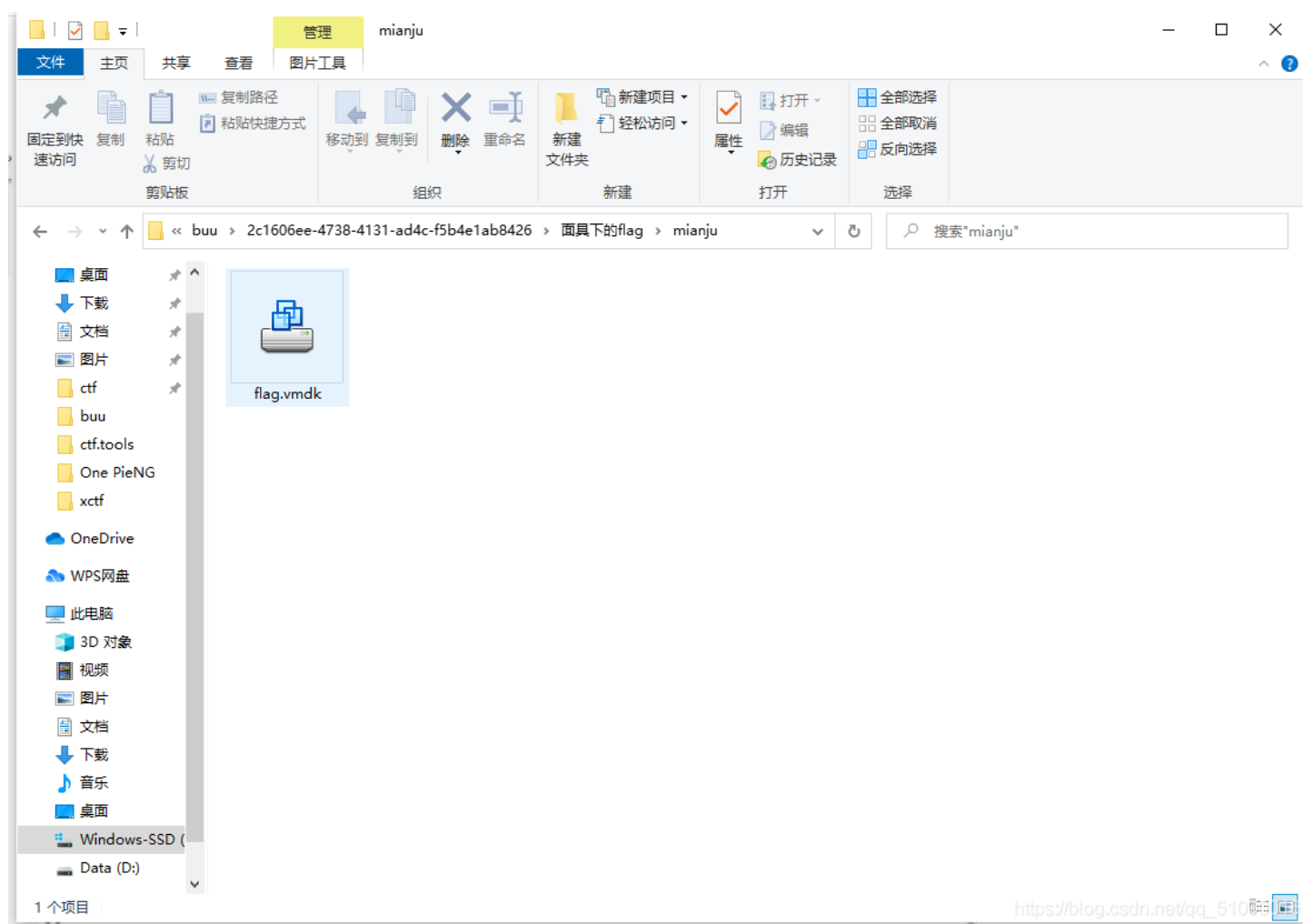
```
$cookiepath = '/';  
// cookie 有效期  
$cookielife = 86400;  
<
```

果然发现了

面具下的flag(用7z解压缩vmdk文件)

先试用O10打开图片，发现里面藏着文件，然后就改成zip后缀试试

得到了这个



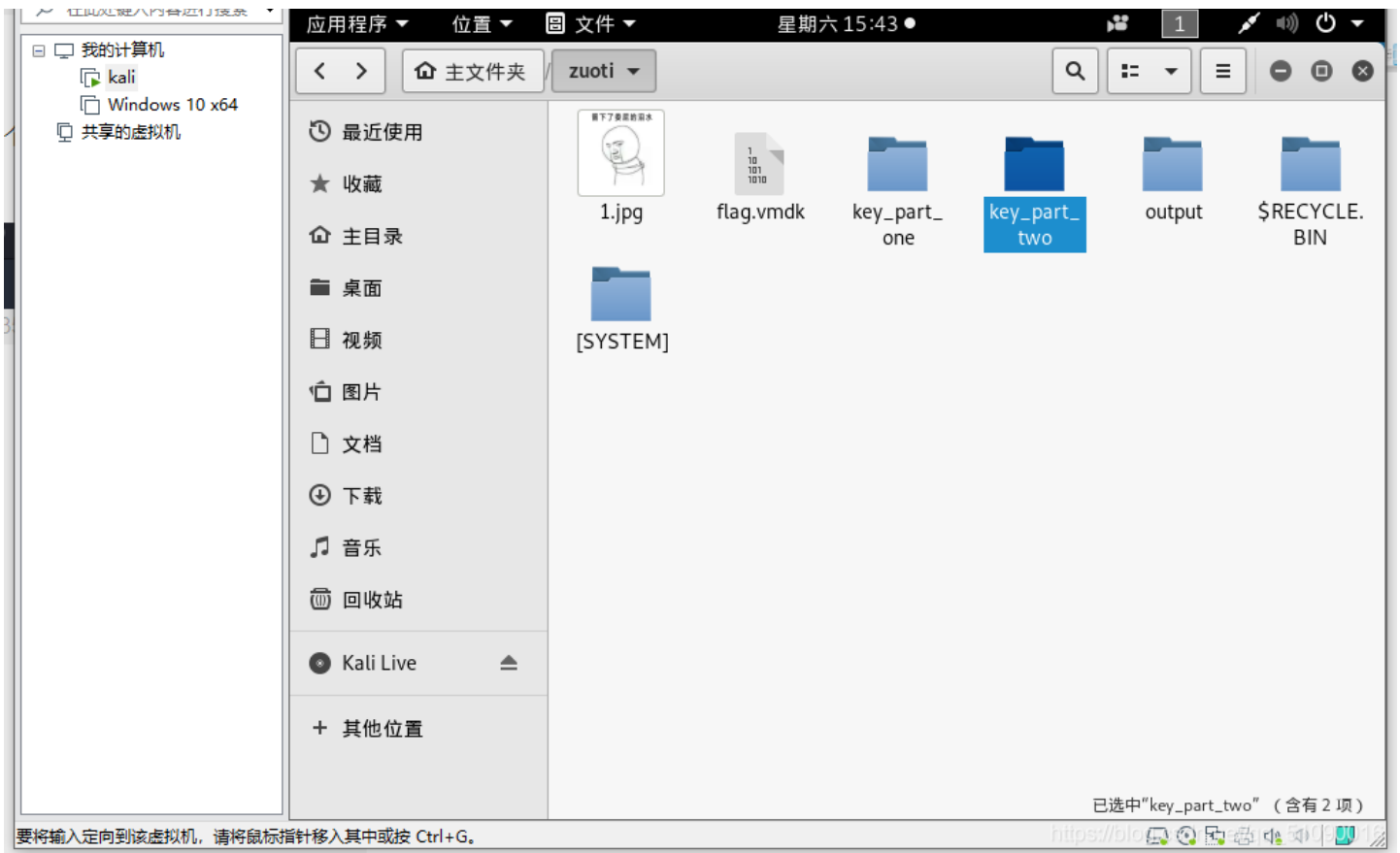
到这我就没思路了。。看wp做的后面

再kali用7z解压缩这个文件（我之前也不知道7z是什么），反正就用这个命令就能解压缩：

```
root@kali: ~/Desktop/temp  
root@kali:~/Desktop/temp# 7z x flag.vmdk -o./
```

然后就得到一堆文件，每个都看看，看到两个关键文件



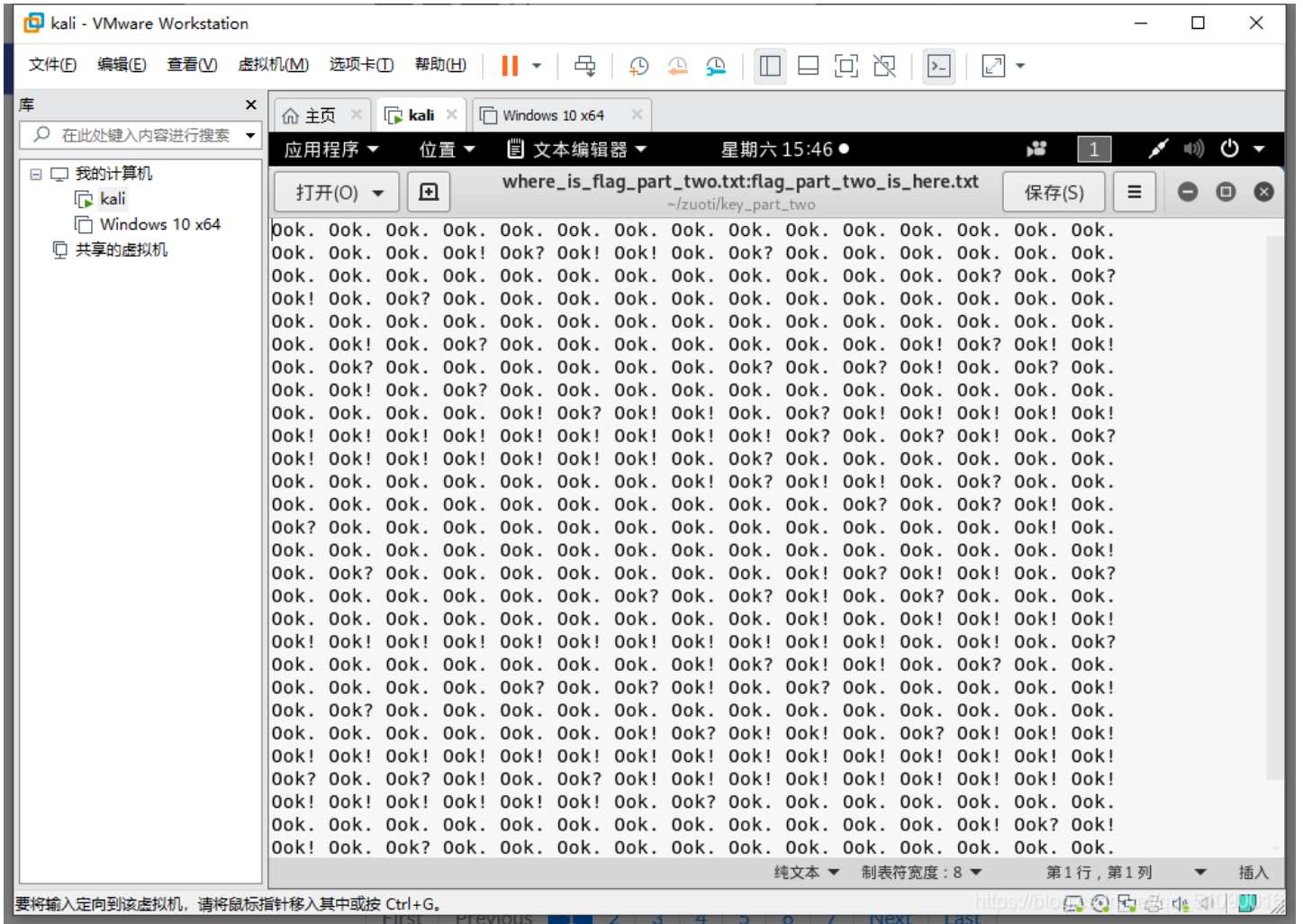


第一个长这样



第二步是key_part_two

第二个长这样：

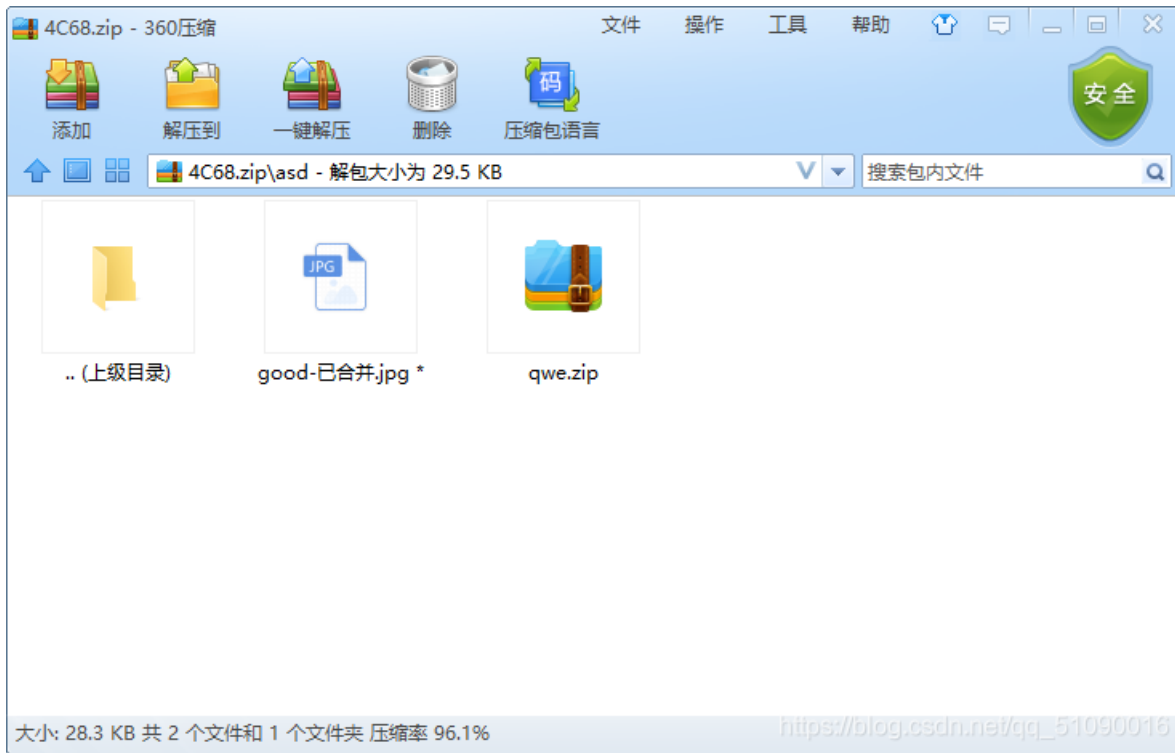


All the hard work (like actually understanding how those lar and his Brainfuck interpreter in PHP

```
_i5_funny!}
```

九连环 (steghide)

显示010里面发现有flag.txt文件，然后使用binwalk foremos大法分离出一个压缩包和一个图片



图片损坏了解压不了，压缩包点开需要密码，先看看是不是伪加密

果然，

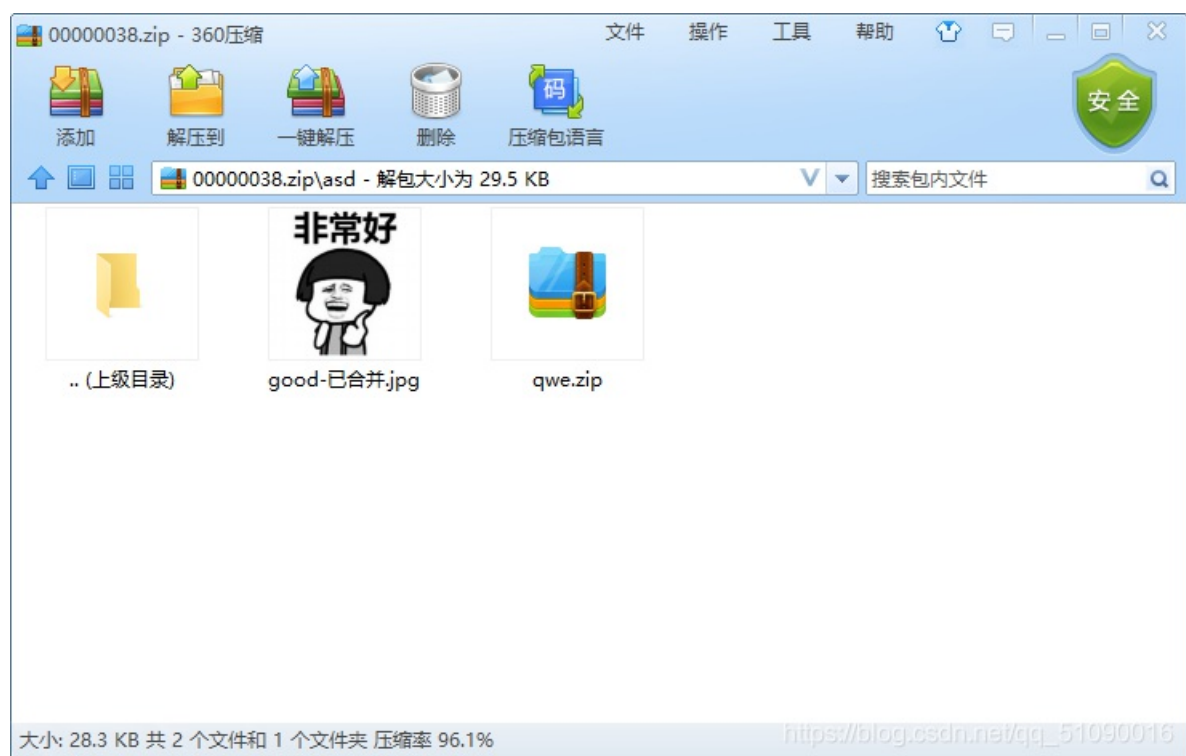
The screenshot shows the 010 Editor interface with a hex dump of a ZIP file. The search results pane at the bottom shows 10 occurrences of the hex value '504b' at addresses 0h, 22h, and 70DEh. The hex dump shows the following data:

Address	Hex	ASCII
7180h	67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18	g.txt.....
7190h	00 29 39 FE E9 7C 48 D3 01 D9 46 44 DC 7C 48 D3)9pé HÓ.ÛFDÛ HÓ
71A0h	01 D9 46 44 DC 7C 48 D3 01 50 4B 05 06 00 00 00	.ÛFDÛ HÓ.PK.....
71B0h	00 01 00 01 00 5A 00 00 00 48 00 00 00 00 00 50Z...H....P
71C0h	4B 01 02 3F 00 0A 00 00 08 00 00 AE 54 53 4B 00	K.?......@TSK.
71D0h	00 00 00 00 00 00 00 00 00 00 00 04 00 24 00 00\$.
71E0h	00 00 00 00 00 10 00 00 00 00 00 00 00 61 73 64asd
71F0h	2F 0A 00 20 00 00 00 00 00 01 00 18 00 69 B8 48	/.....i.H
7200h	34 83 48 D3 01 69 B8 48 34 83 48 D3 01 E9 FC 59	4fHÓ.i.H4fHÓ.éüY
7210h	31 83 48 D3 01 50 4B 01 02 3F 00 14 00 08 08	lfHÓ.PK.?......
7220h	00 48 4E 53 4B 8C 3A D5 7E 88 70 00 00 28 75 00	.HNSKÖ:Ö~^p..(u.
7230h	00 16 00 24 00 00 00 00 00 00 00 20 00 00 00 22	...\$.
7240h	00 00 00 61 73 64 2F 67 6F 6F 64 2D E5 B7 B2 E5	...asd/good-â~â
7250h	90 88 E5 B9 B6 2E 6A 70 67 0A 00 20 00 00 00 00	.â~q.jpg..
7260h	00 01 00 18 00 69 31 23 9C 7C 48 D3 01 29 AE F6il#æ HÓ.)@8
7270h	8F 82 48 D3 01 89 7E E8 D2 7C 48 D3 01 50 4B 01	.,HÓ.æ~èò HÓ.PK.
7280h	02 3F 00 0A 00 00 08 00 00 F1 52 53 4B D3 13 C6	.?......ñRSKÖ.Æ
7290h	E0 B8 00 00 00 B8 00 00 00 0B 00 24 00 00 00 00	à.....\$.
72A0h	00 00 00 20 00 00 00 DE 70 00 00 61 73 64 2F 71Ep..asd/q
72B0h	77 65 2E 7A 69 70 0A 00 20 00 00 00 00 00 01 00	we.zip..
72C0h	18 00 D9 DB B7 42 81 48 D3 01 39 D5 F6 8F 82 48	.ÛÛ.B.HÓ.9öö.,H
72D0h	D3 01 49 83 5B 0F 81 48 D3 01 50 4B 05 06 00 00	Ö.If ..HÓ.PK.....
72E0h	00 00 03 00 03 00 1B 01 00 00 BF 71 00 00 00 00zq....
72F0h		

The search results pane shows the following data:

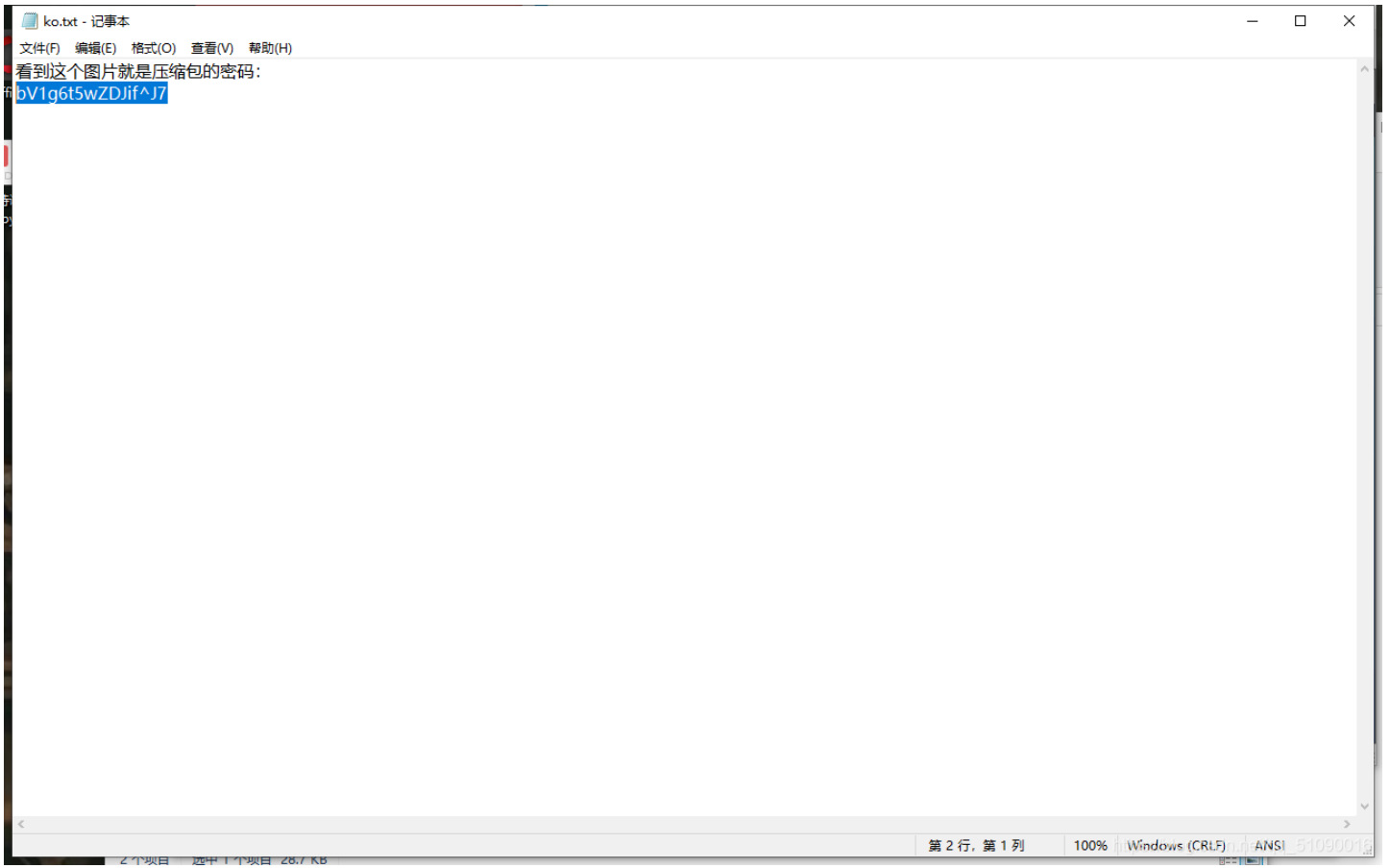
地址	值
0h	504b
22h	504b
70DEh	504b

这样就能正常解压了

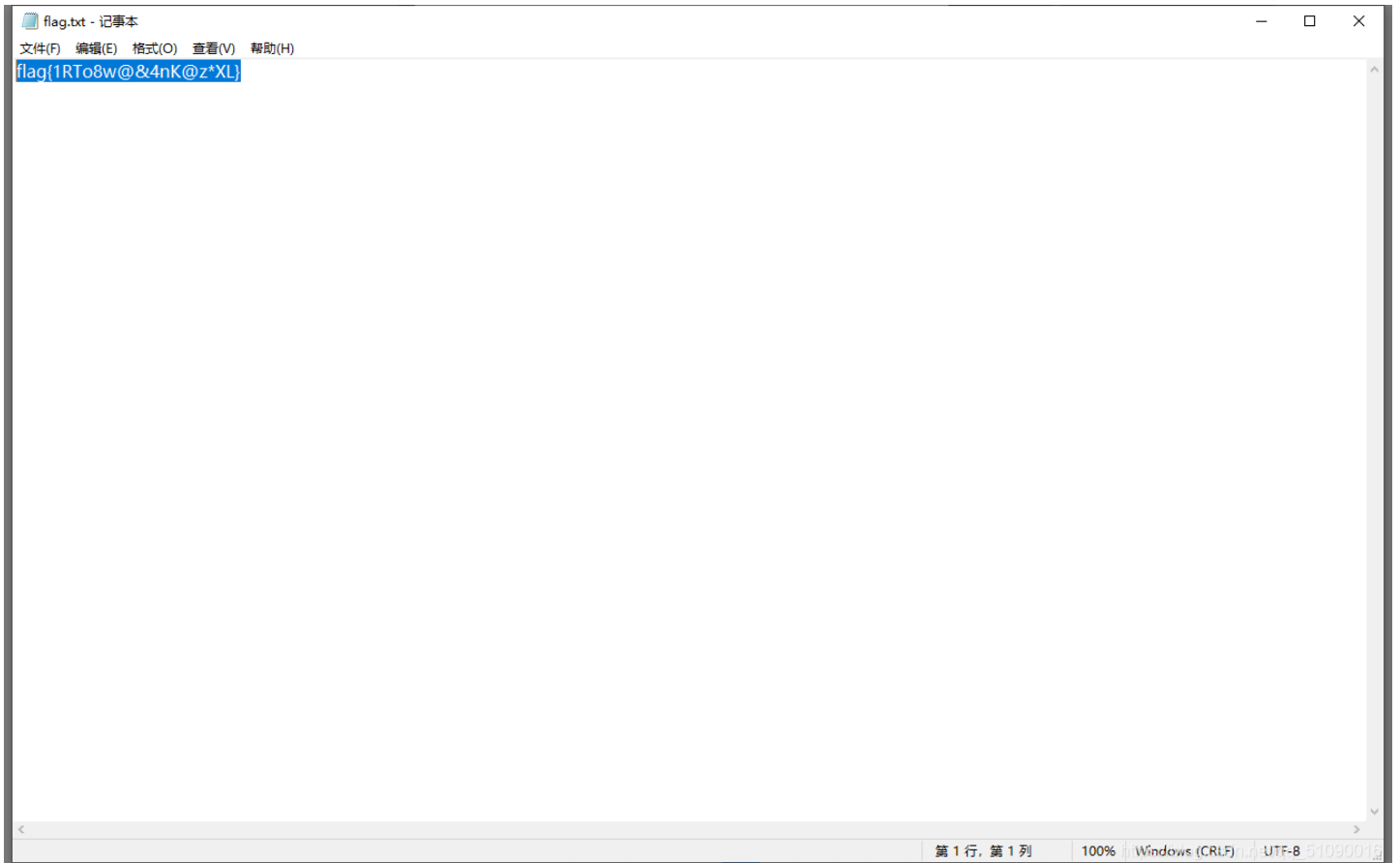


但是另一个压缩包也需要密码，这肯定不是伪加密了，关键应该在图片上：这里涉及到steghide的使用

使用 `steghide extract -sf good.jpg`，空密码即可

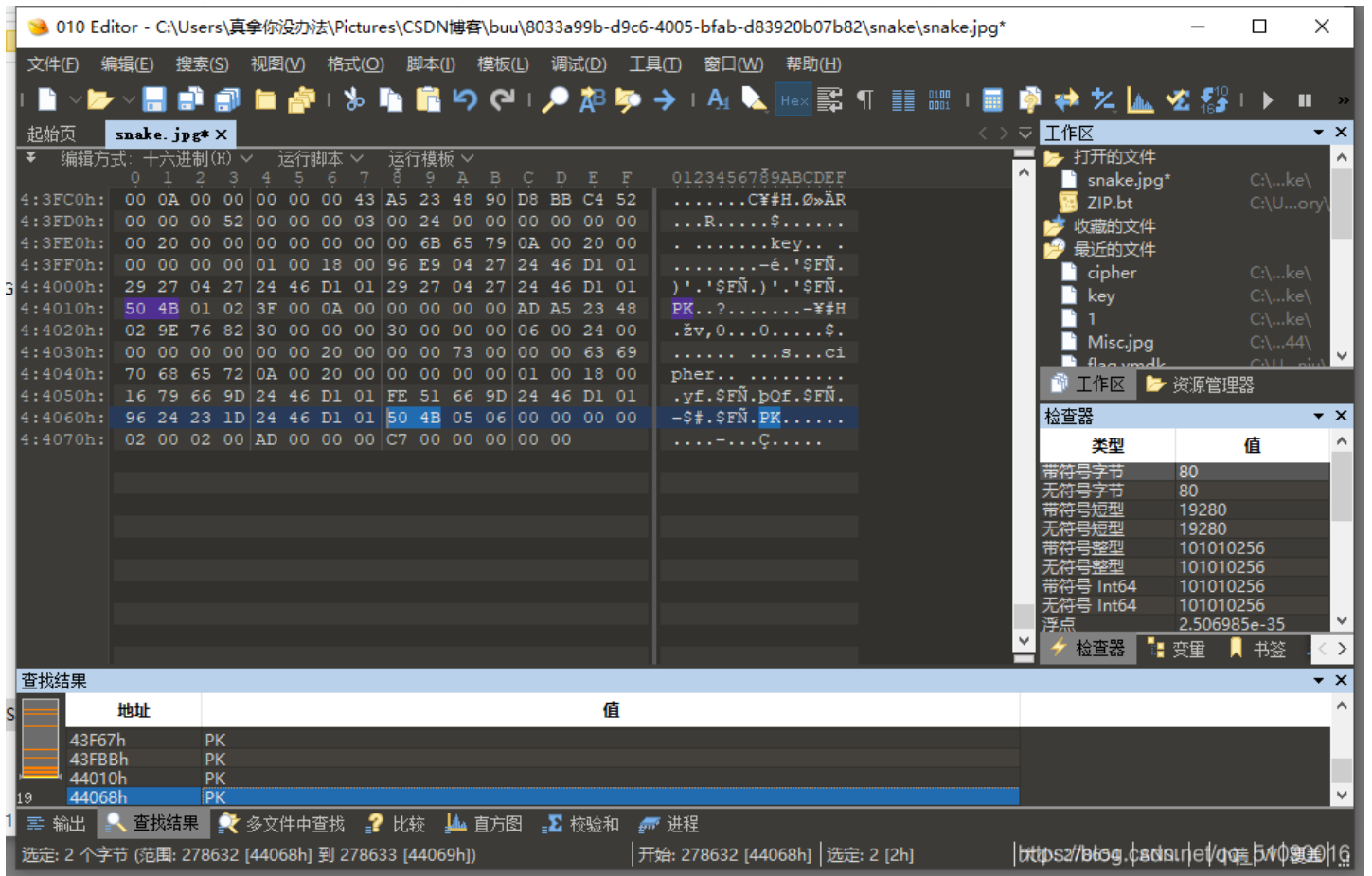


解压得到的txt文件

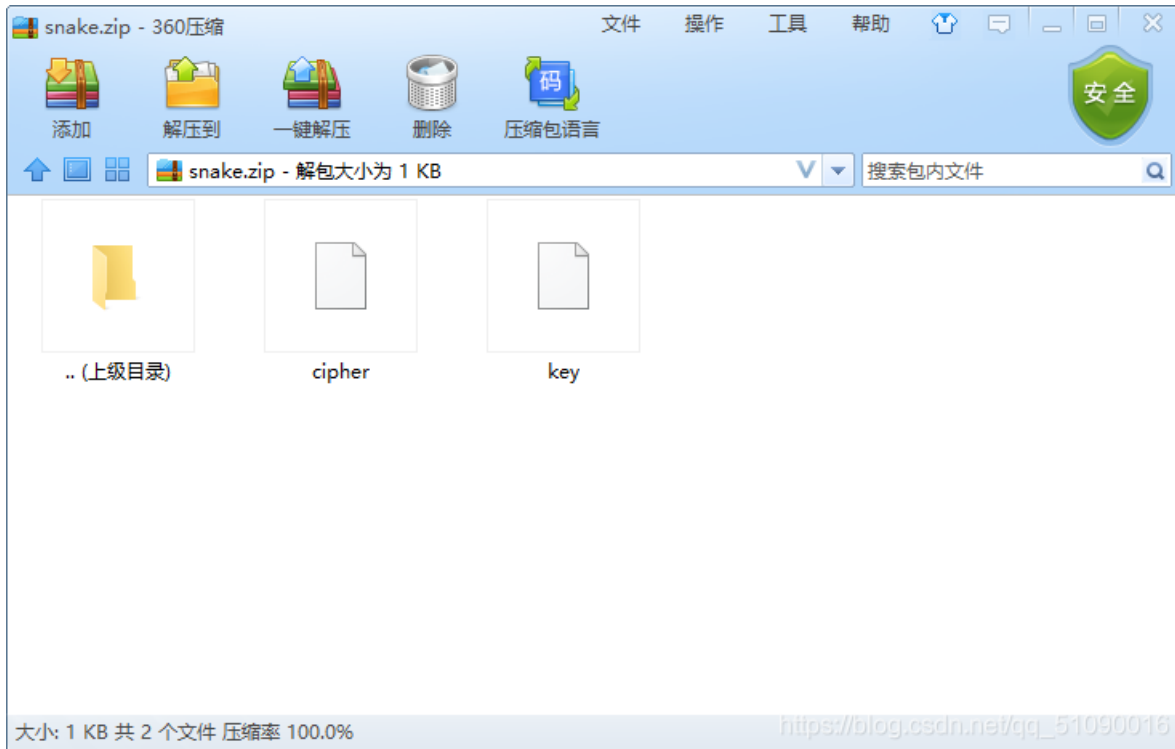


snake (serpent解密)

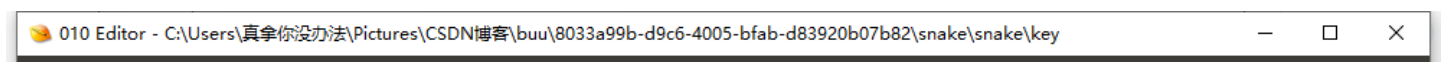
附件用010打开看看，搜索下flag txt pk等等

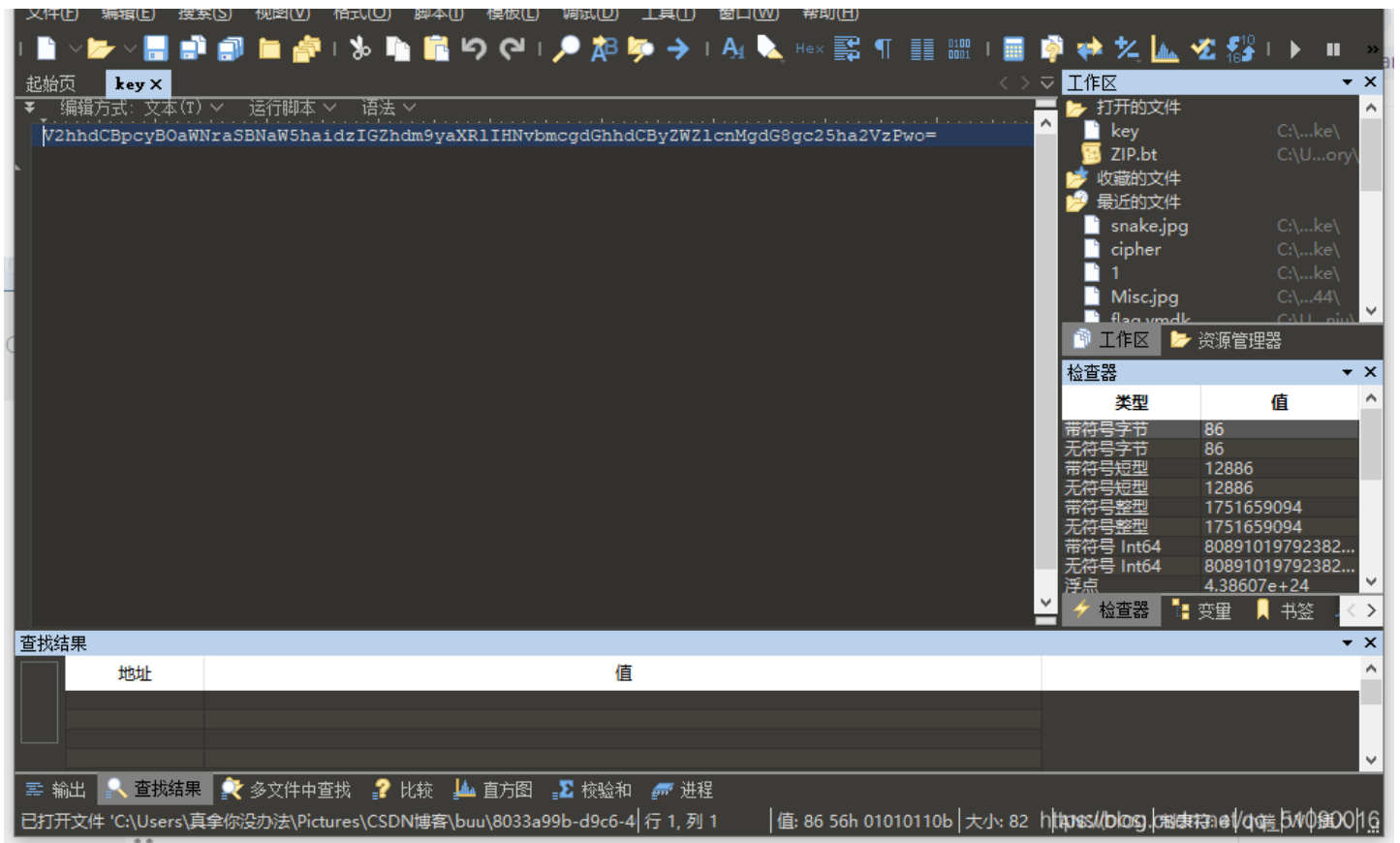


里面应该是有压缩文件，改成zip看看



果然有，先看key






base64解密:



这我哪知道，百度一下是anaconda，然后就是解密了，是什么解密呢？题目是snake，解密应该和这个有关，搜了一下才知道还有serpent解密，网址贴这

 Key is not valid hexadecimal string. Permitted characters are: [a-fA-F0-9 \-] and the string must have even length.

Input type: File

File: Browse

Function: SERPENT

Mode: ECB (electronic codebook)

Key: (hex)

Plaintext Hex

> Encrypt! > Decrypt! ▶ 🔗

100%
File was uploaded.

Decrypted text:

00000000	43	54	46	7b	77	68	6f	5f	6b	6e	65	77	5f	73	65	72
00000010	70	65	6e	74	5f	63	69	70	68	65	72	5f	65	78	69	73
00000020	74	65	64	7d	00	00	00	00	00	00	00	00	00	00	00	00

[Download as a binary file](#) [?]

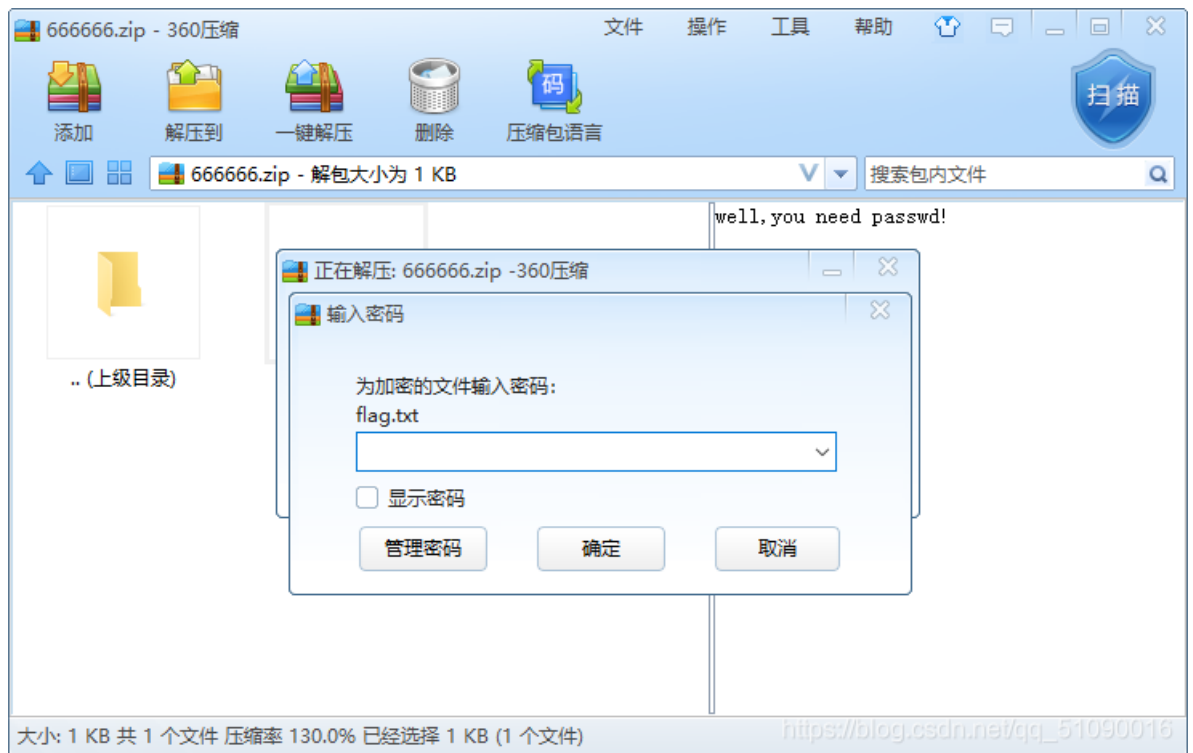
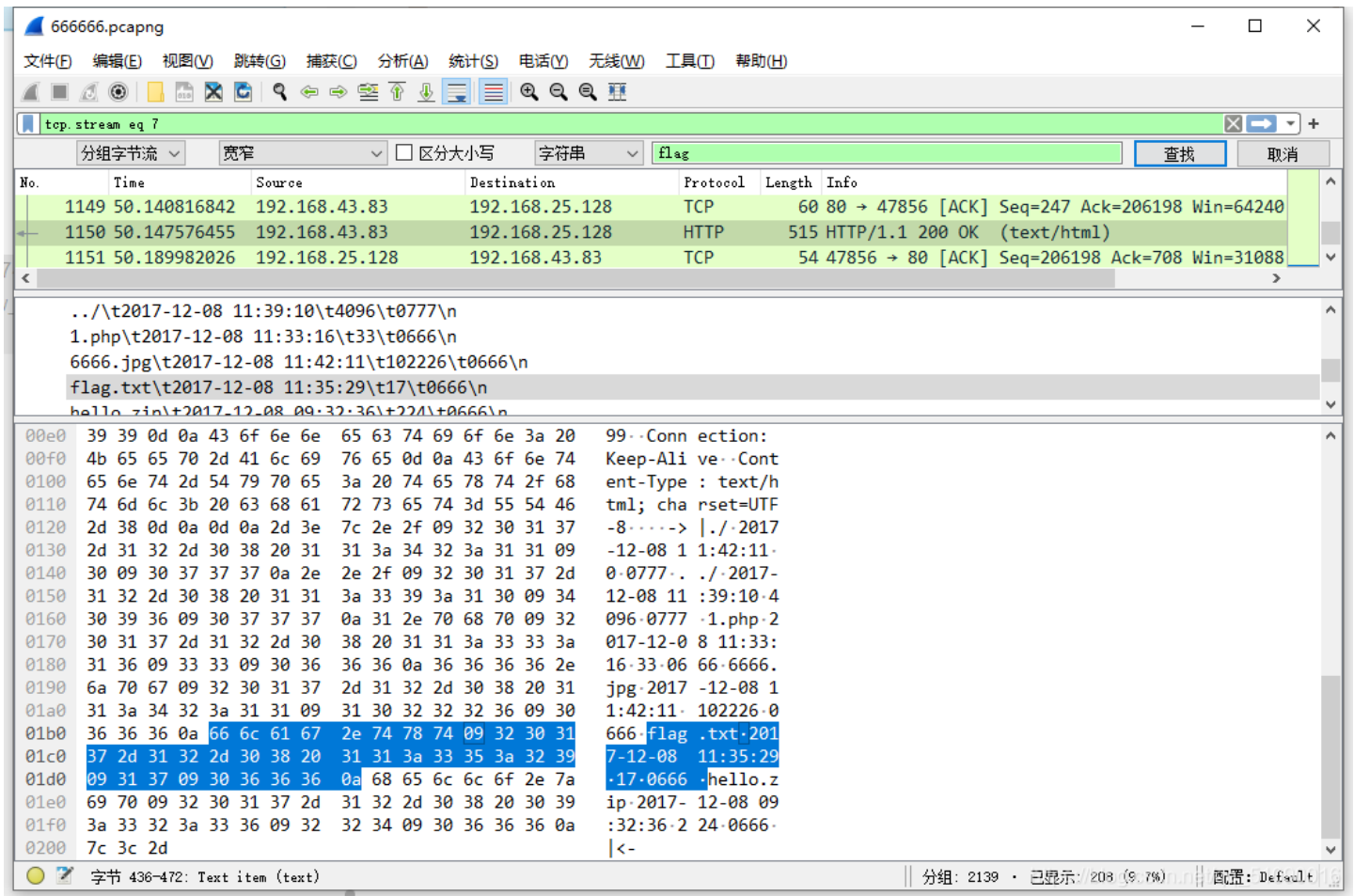
C	T	F	{	w	h	o	_	k	n	e	w	_	s	e	r
p	e	n	t	_	c	i	p	h	e	r	_	e	x	i	s
t	e	d	}

https://blog.csdn.net/qq_51090016 Inactive

这样就有了

菜刀666（流量分析）

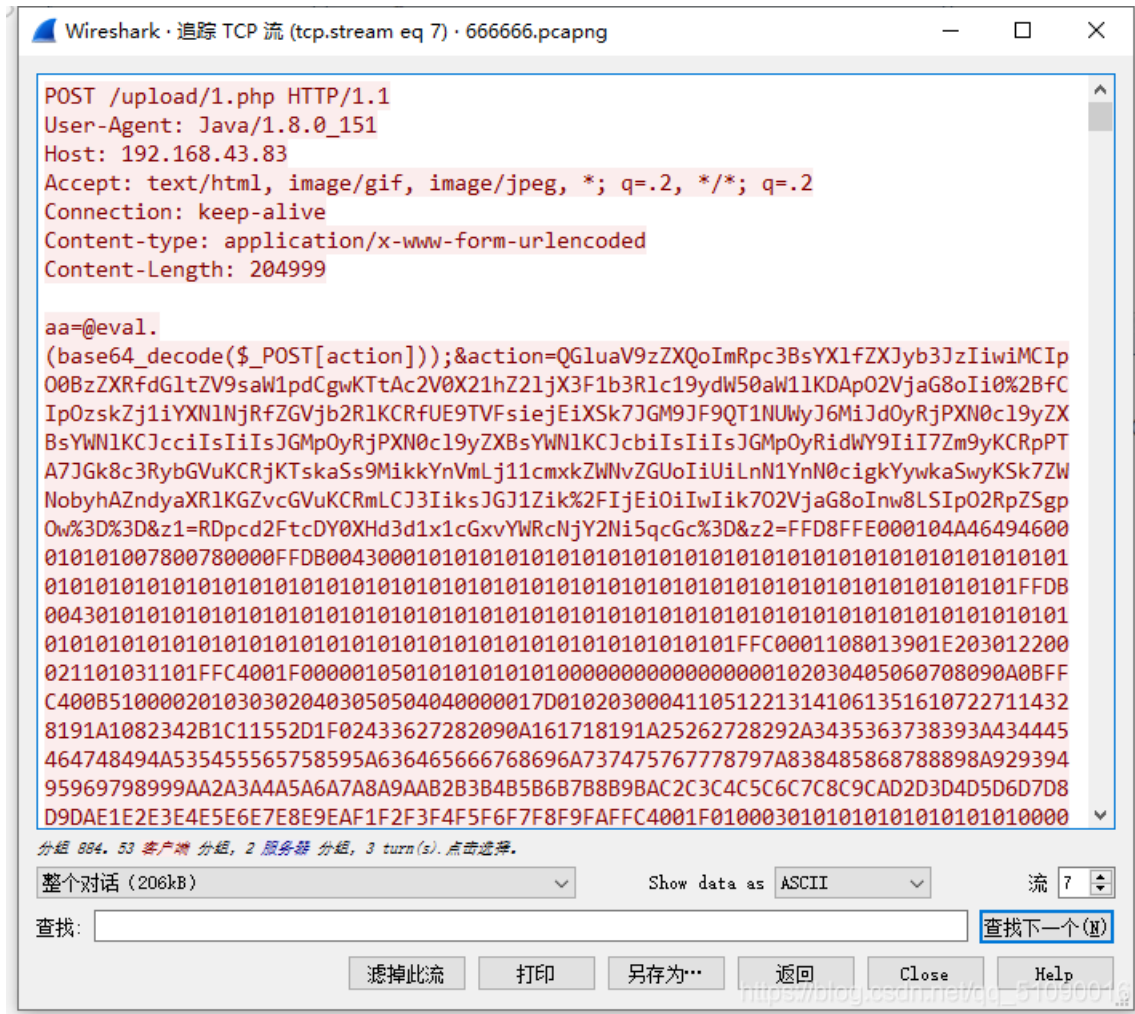
首先是很常规的套路，用winshark打开，搜索flag，发现有个txt文件藏在里面



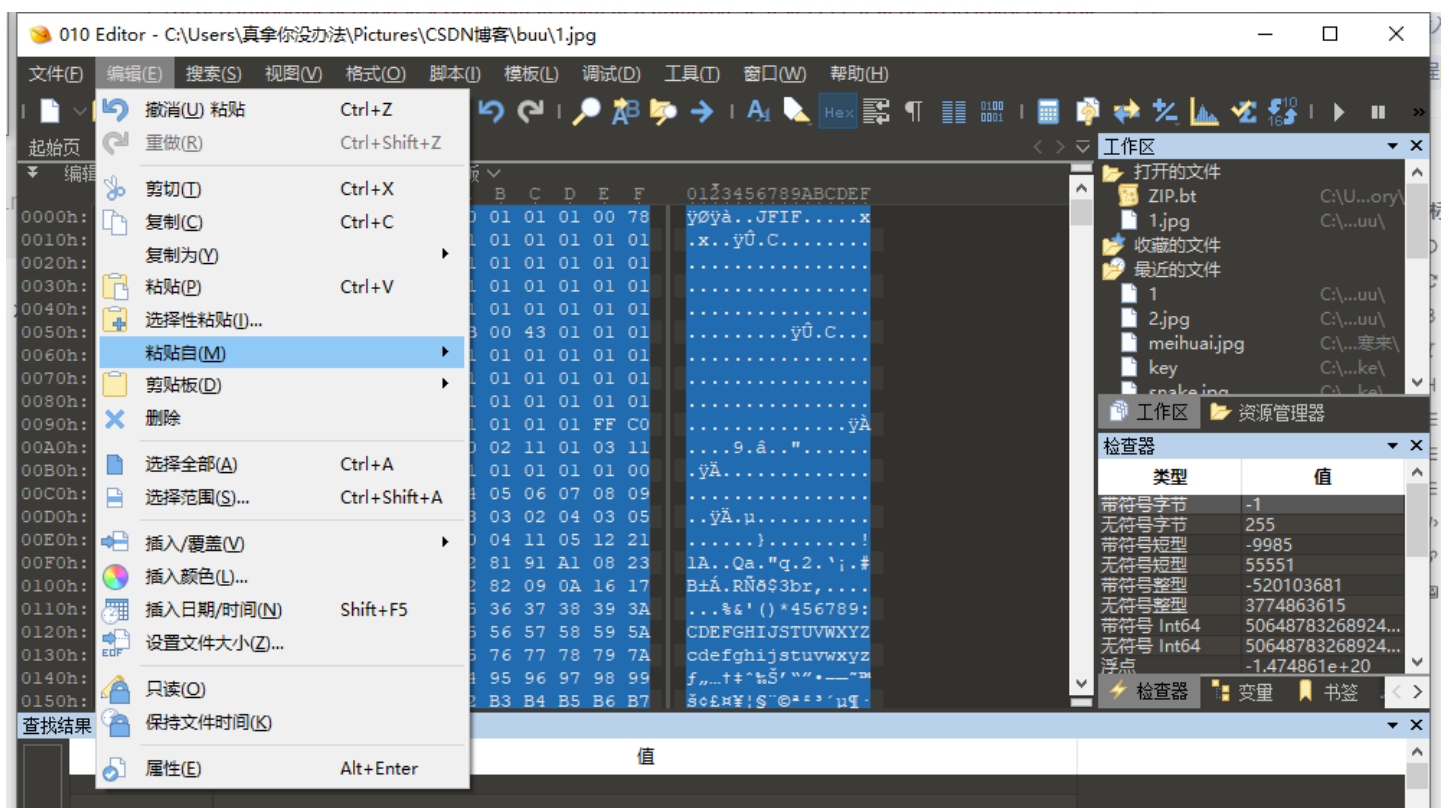
后缀改成zip打开看看

需要密码，这时候就要想到从本身的文件入手了，搜索一下password。。。没有，那tcp追踪流看看

看到7流的时候发现一串16进制字符



又看到有个z1 z2, z1我还以为是base, 结果不是, 先看z2吧 FF D8开头FF D9结尾, 判断为jpg图片, 将这些十六进制复制出来, 粘贴到010里面, 注意具体操作如图, 要粘贴自16进制文件



010 Editor - C:\Users\真拿你没办法\Pictures\CSDN博客\buu\1.jpg

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

输出 查找结果 多文件中查找 比较 直方图 校验和 进程

开始: 0 [0h] | 选定: 102226 [18F52h] | 大小: 102226h

文件类型也是16进制:

010 Editor - C:\Users\真拿你没办法\Pictures\CSDN博客\buu\1.jpg

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

Hex

编辑方式: 十六进制(H) 运行脚本 运行模板

文本(T) 十六进制(H) 二进制(I) 脚本(S) 模板(T) EBDCIC(B) Unicode(U) UTF-8(8) 驱动器(R) 进程(P)

```
00000000: 00 10 4A 46 49 46 00 01 01 01 00 78 01 23 45 67 89 ABCDEF y0yà..JFIF....x
00000001: FF DB 00 43 00 01 01 01 01 01 01 01 .x.ÿÛ.C.....
00000002: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000003: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000004: 01 01 01 01 01 01 FF DB 00 43 01 01 .....ÿÛ.C...
00000005: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000006: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000007: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000008: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000009: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
0000000A: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
0000000B: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
0000000C: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
0000000D: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
0000000E: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
0000000F: 01 01 01 01 01 01 01 01 01 01 01 01 .....ÿÛ.C...
00000010: 00 00 00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 00 00 01 05 01 01 01 01 01 01 00
```

查找结果

地址	值



密码有了

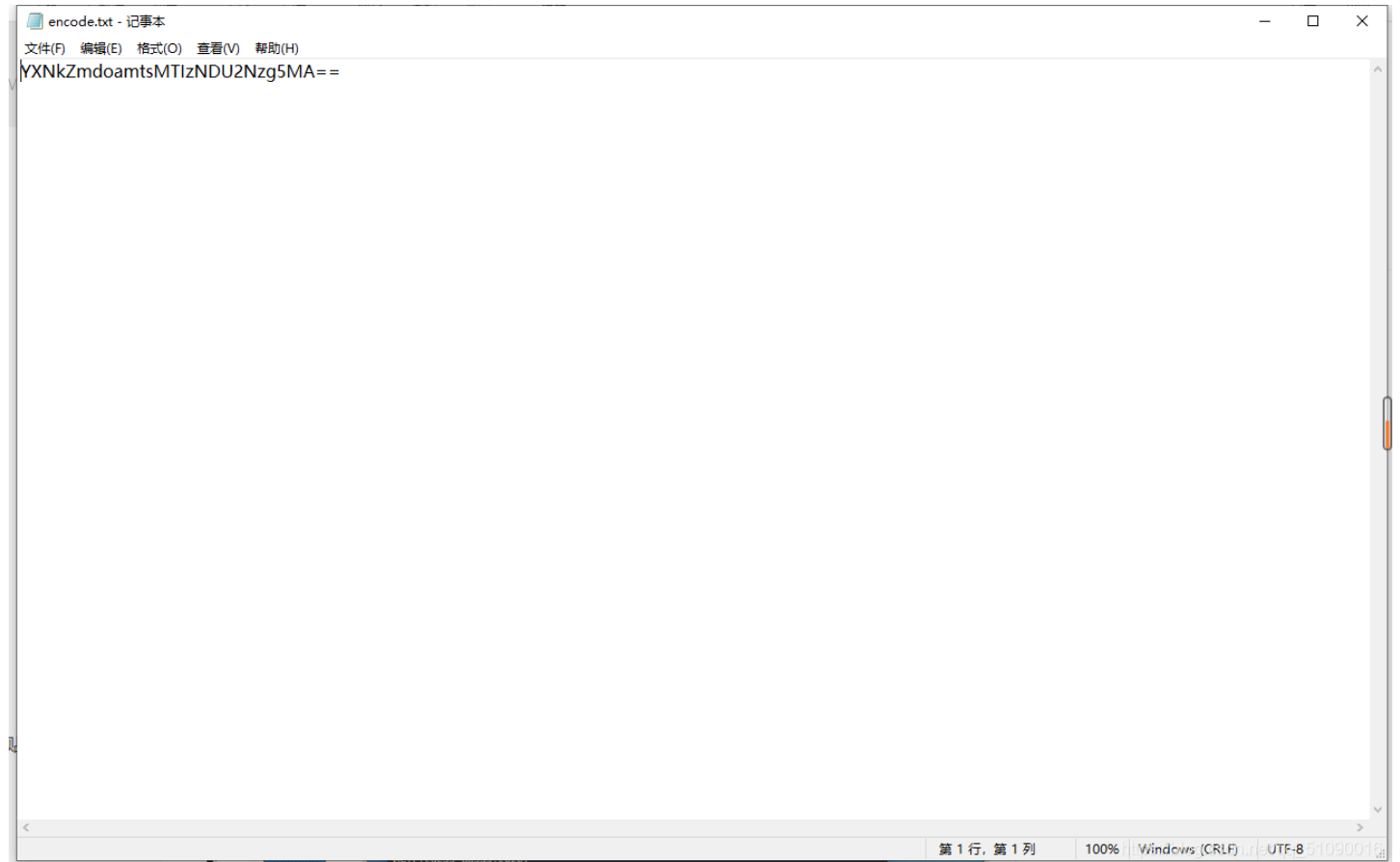
flag.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}

[SWPU2019]神奇的二维码（binwalk -e分离）

正常010打开，发现有rar文件，先试试改成rar文件，解压缩得到

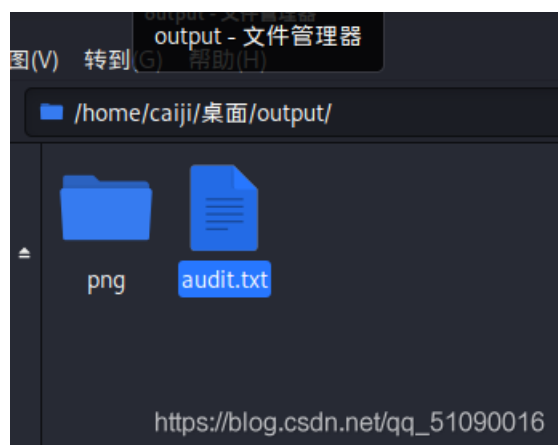


解码得到

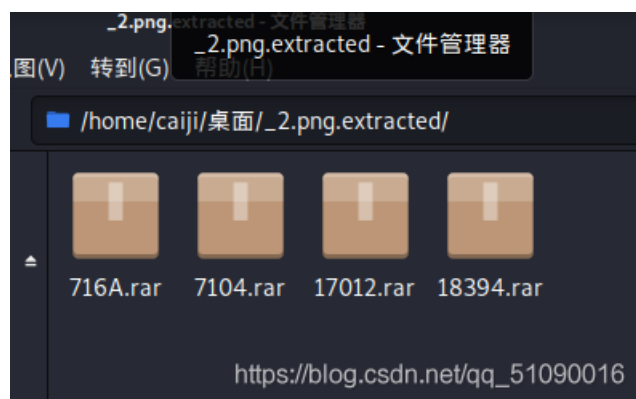


还以为这就是flag。。没思路了，直接看wp

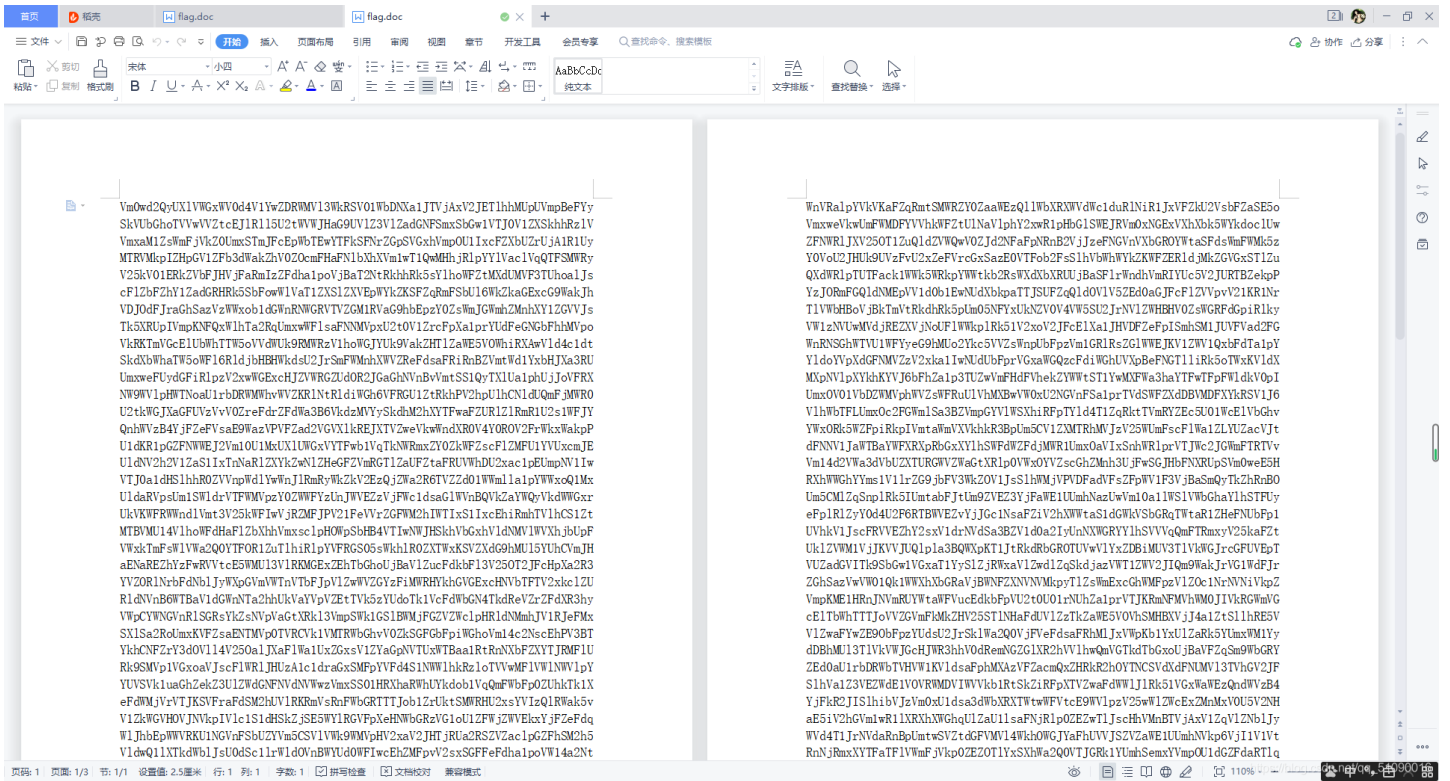
放到虚拟机里binwalk一下 再foremost一下



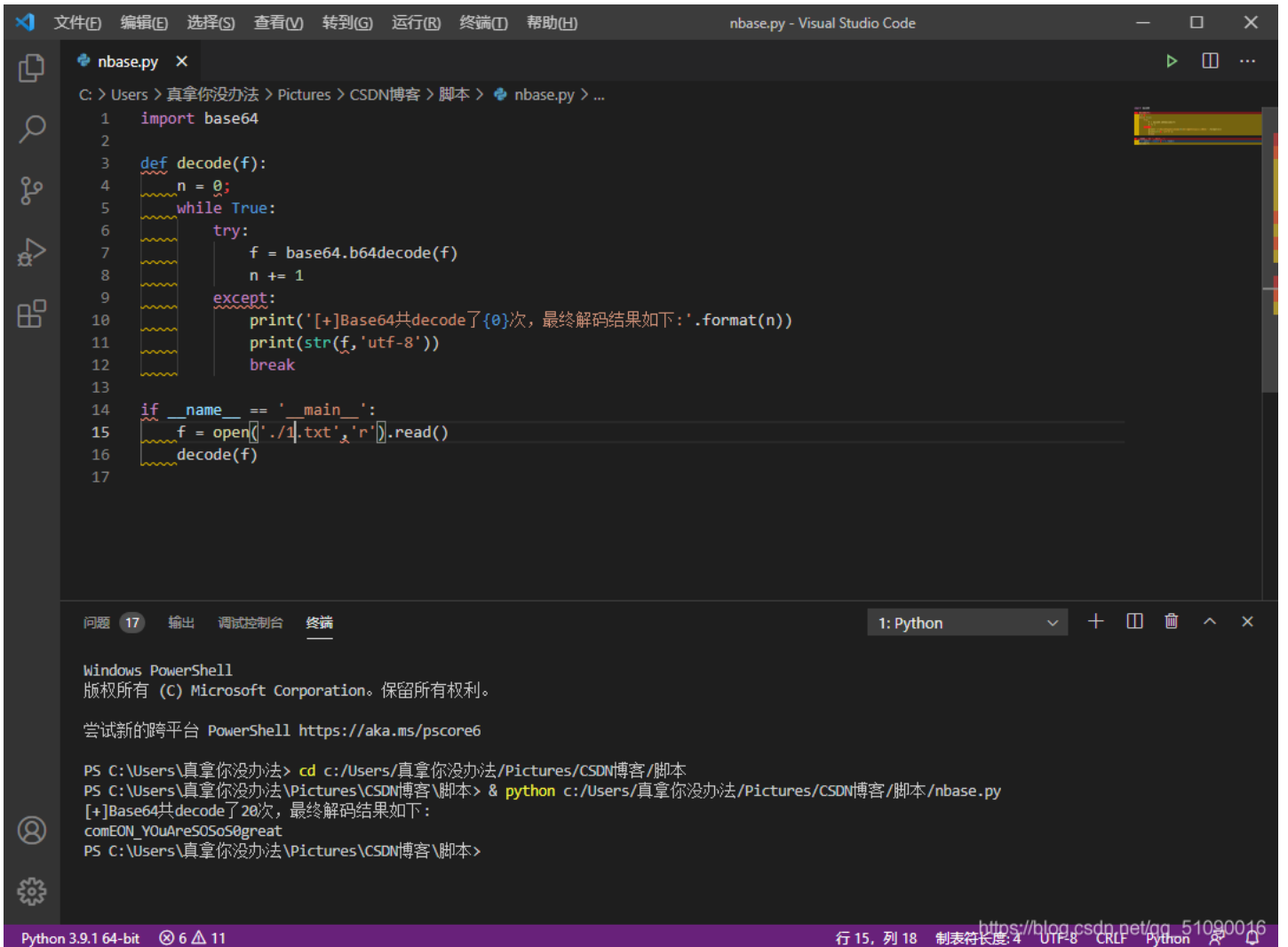
用binwalk -e试一下



分离出了四个压缩包，发现有一个需要密码。。试了下发现其实asdfghjkl1234567890是看看flag在不在里面-.rar的密码
其实这里面什么都没有，就是单纯的图片，什么都没有隐写...浪费我时间...

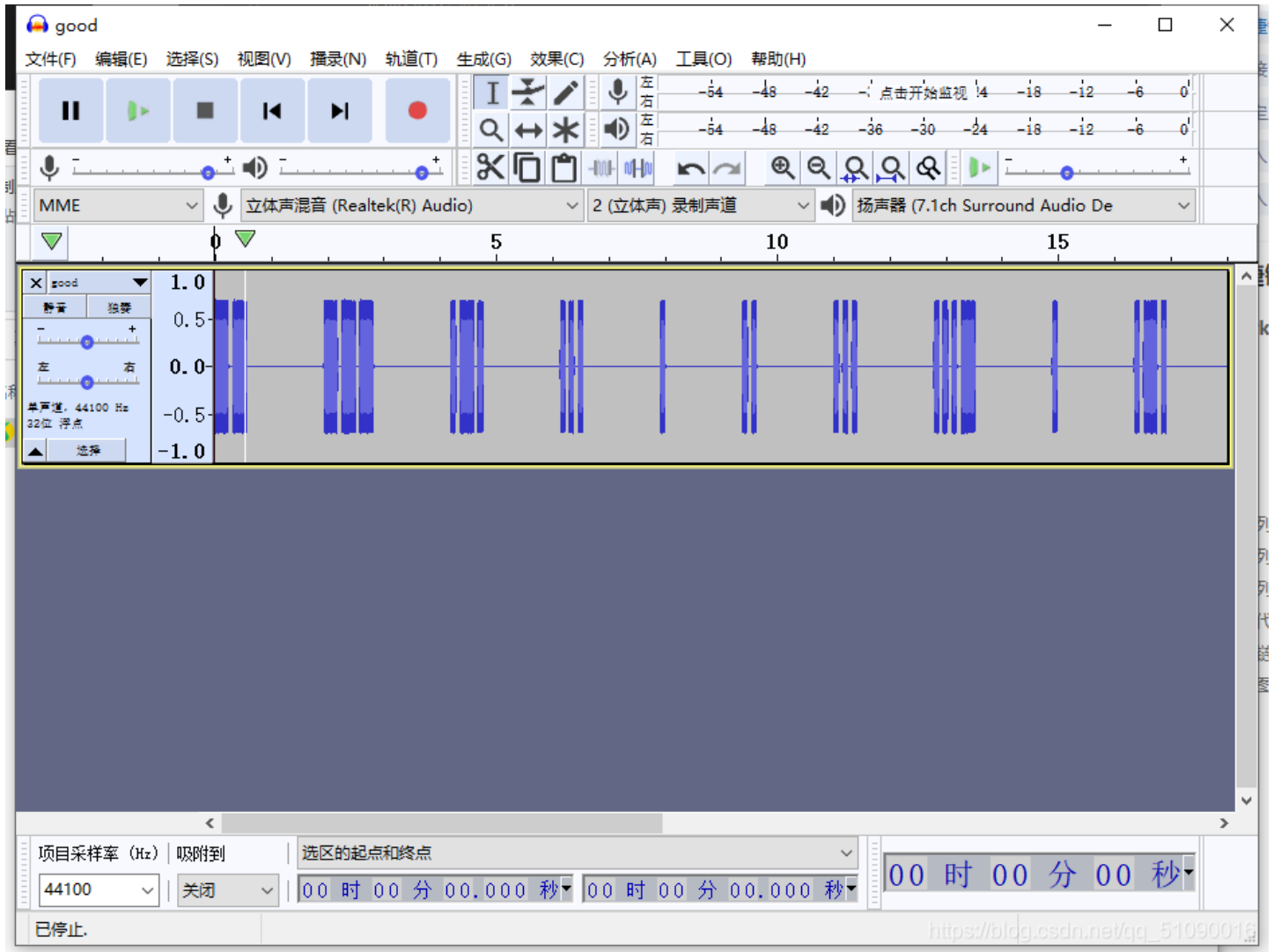


一大串。。应该被编码了很多次，用脚本



https://blog.csdn.net/gg_51090016

解压得到音频文件，使用Audacity打开



摩斯电码

英文字母:

MORSEISVERYVEREASY

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

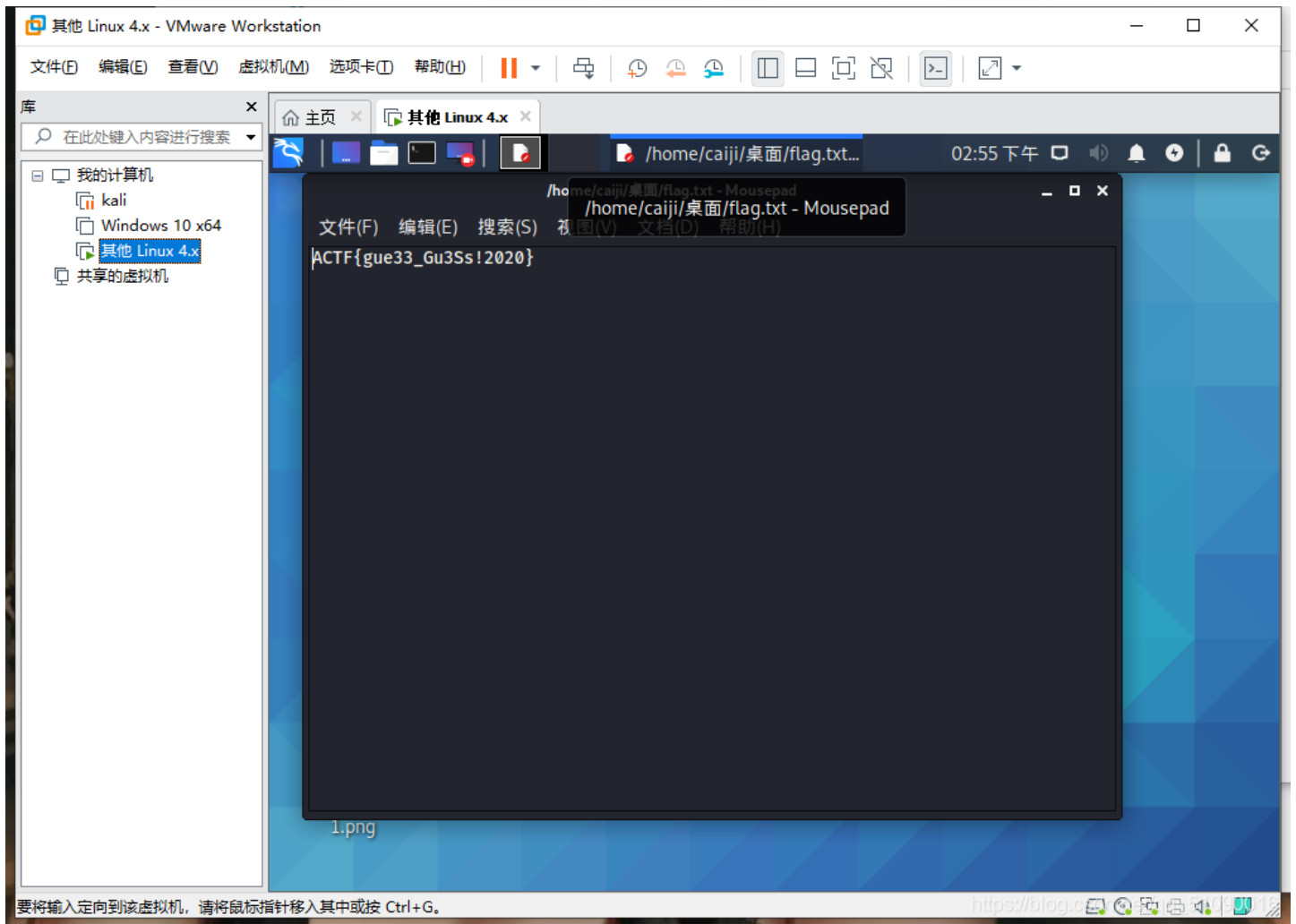
摩斯电码: (格式要求: 可用空格或单斜杠/来分隔摩斯电码, 但只可用一种, 不可混用)

[ACTF新生赛2020]outguess (outguess的用法)

解压后发现一堆东西，重点应该还是在图片上，根据提示猜测是outguess的使用，用法贴这里

kali下面输入outguess -k 'abc' -r mmm.jpg flag.txt

得到flag.txt

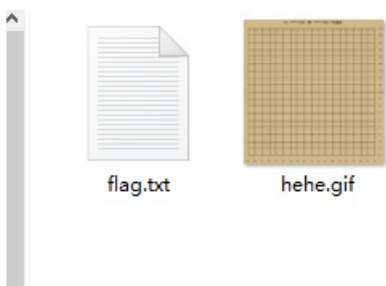


谁赢了比赛？

正常流程，丢进kali

```
root@kali:~/Desktop# binwalk who_won_the_game.png
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          PNG image, 10000 x 10000, 8-bit
erlaced
1430236     0x15D2DC    RAR archive data, version 4.x,
MAIN_HEAD
```

binwalk -e 分离获得压缩包，爆破得到



flag.txt假的。。。

分离gif吧：一直看到三百多张发现了点东西

A B C D E F G H I J K L M N O P Q R S

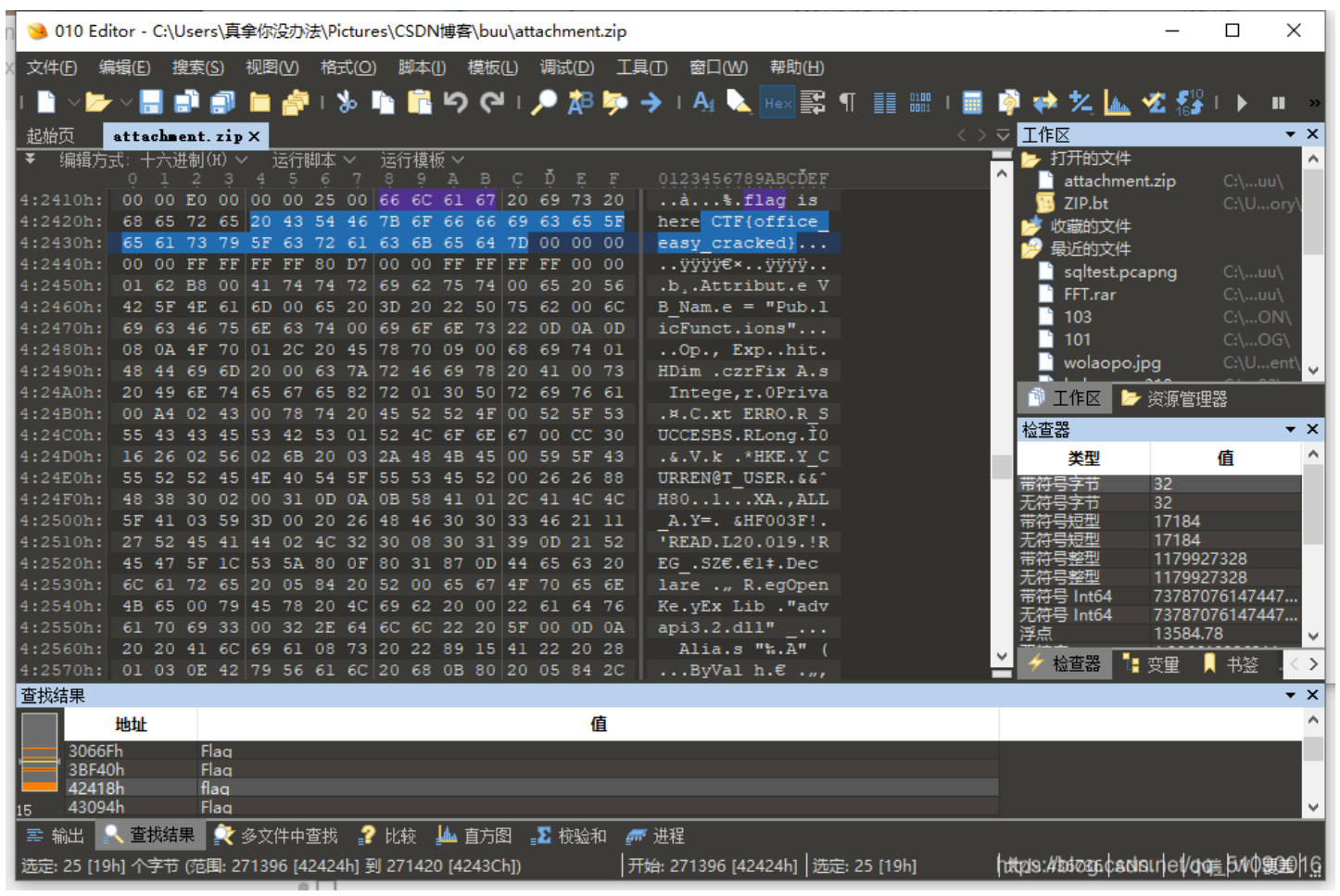
https://blog.do_you_know_where_is_the_flag

stegsolve打开。。换通道，终于有了



[HBNIS2018]excel破解（修改后缀）

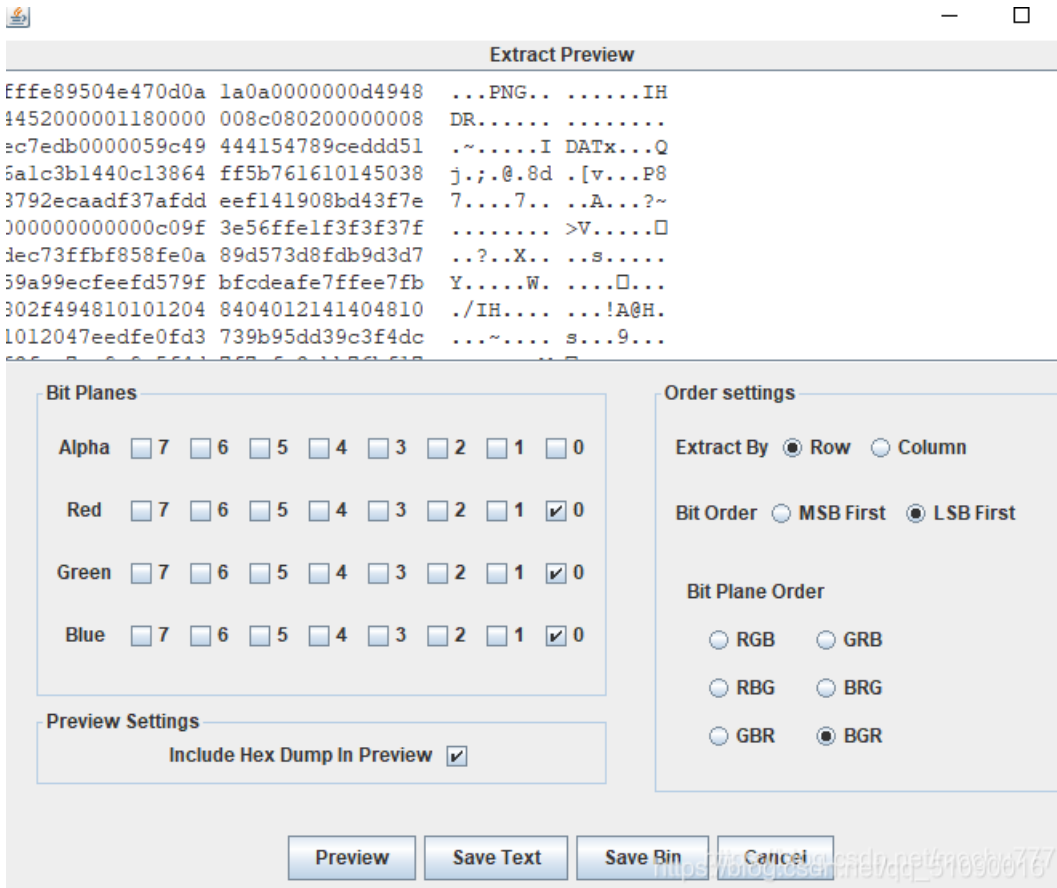
修改zip后缀，然后用010打开。。。就有了??



喵喵喵（奇怪的lsb NTFS文件流隐写）

这题感觉好难

题目提示有二维码，但是010打开并没有发现隐藏压缩包，应该想到lsb隐写
但是谁能想到要设置成这样才行？？



另存为png文件发现打不开。。改一下文件头就好了

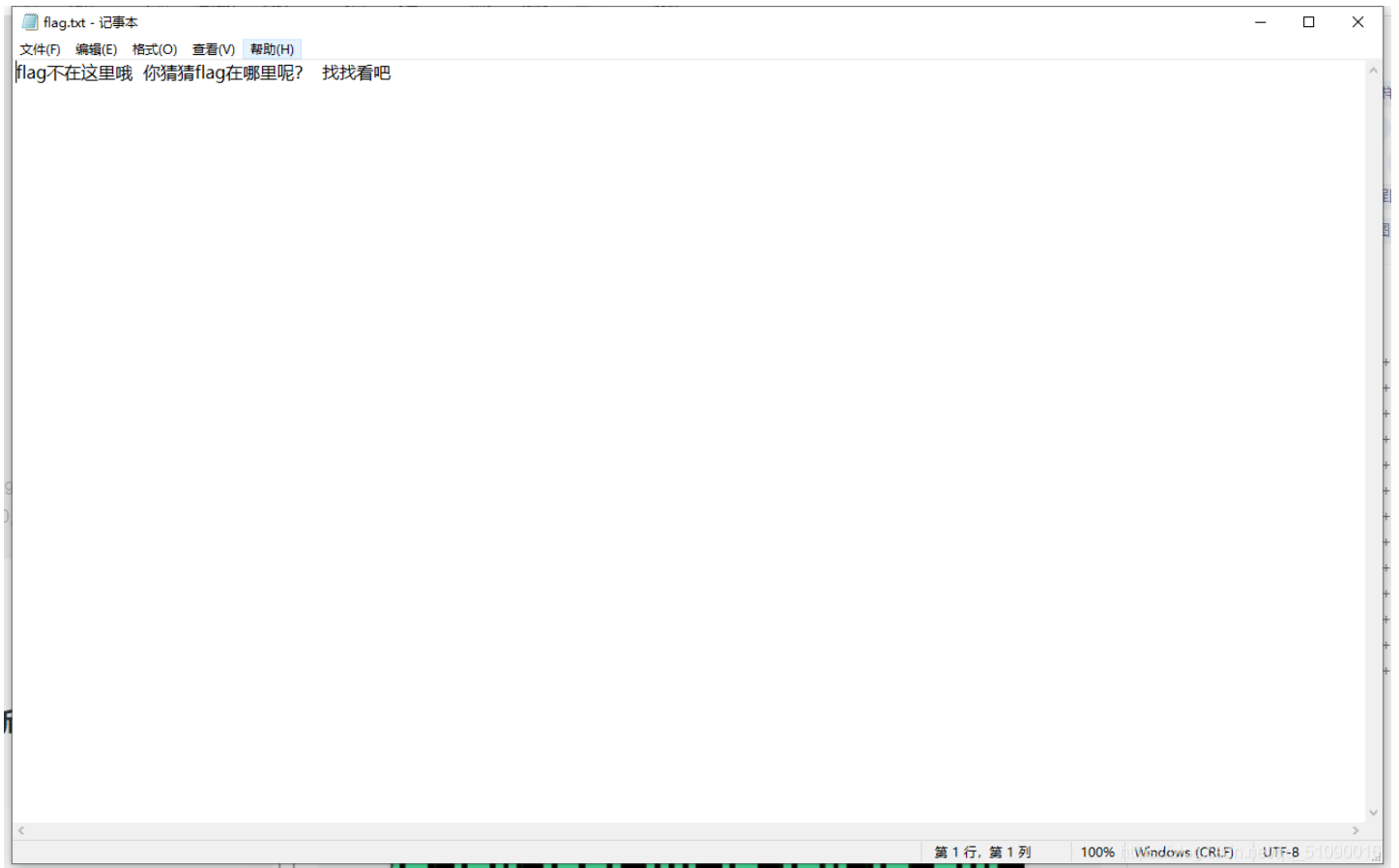


这明显是高的问题了，加个高吧



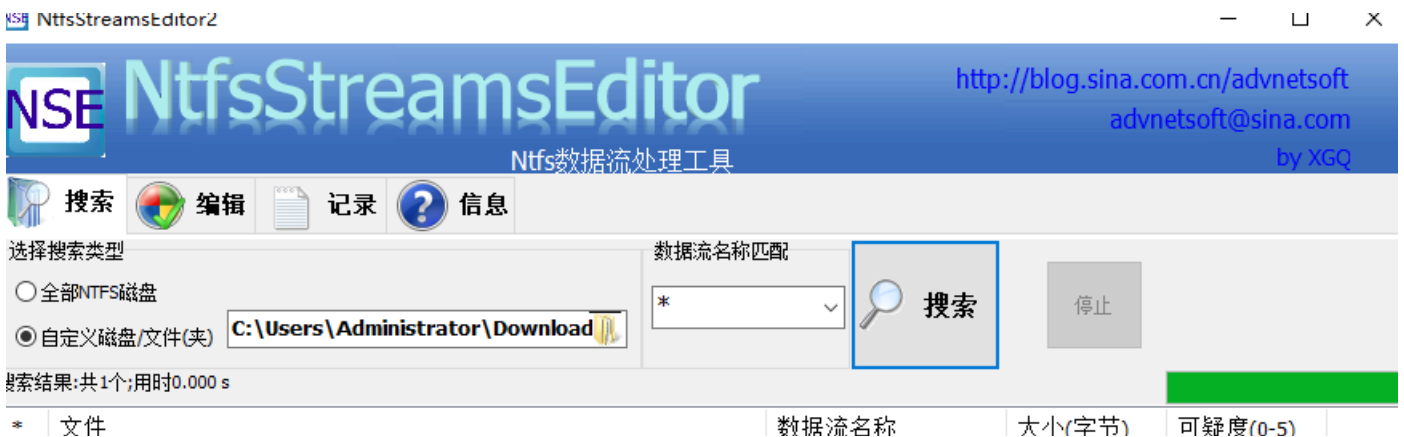


扫了之后是个网盘地址。。下载flag.rar打开



??? 看wp

这里猜测有NTFS文件流隐写，将flag.txt解压到一个新建的文件夹内，利用NtfsStreamsEditor



先是爆破zip3



得到:

从小 5 就 20 列文虎克,

我每年的 7 月 11 日的生日愿望就是拥有一个



提示 520 711

使用Kinovea打开影流之主.mp4



敲击码(Tap code)是一种以非常简单的方式对文本信息进行编码的方法。因该编码对信息通过使用一系列的点击声音来编码而命名，

敲击码是基于5×5方格波利比奥斯方阵来实现的，不同点是是用K字母被整合到C中。

敲击码表：

1	2	3	4	5	
1	A	B	C/K	D	E
2	F	G	H	I	J
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Bash

在第7.36s发现第二段信息：dXBfdXBfdXA=

base解码 `up_up_up`

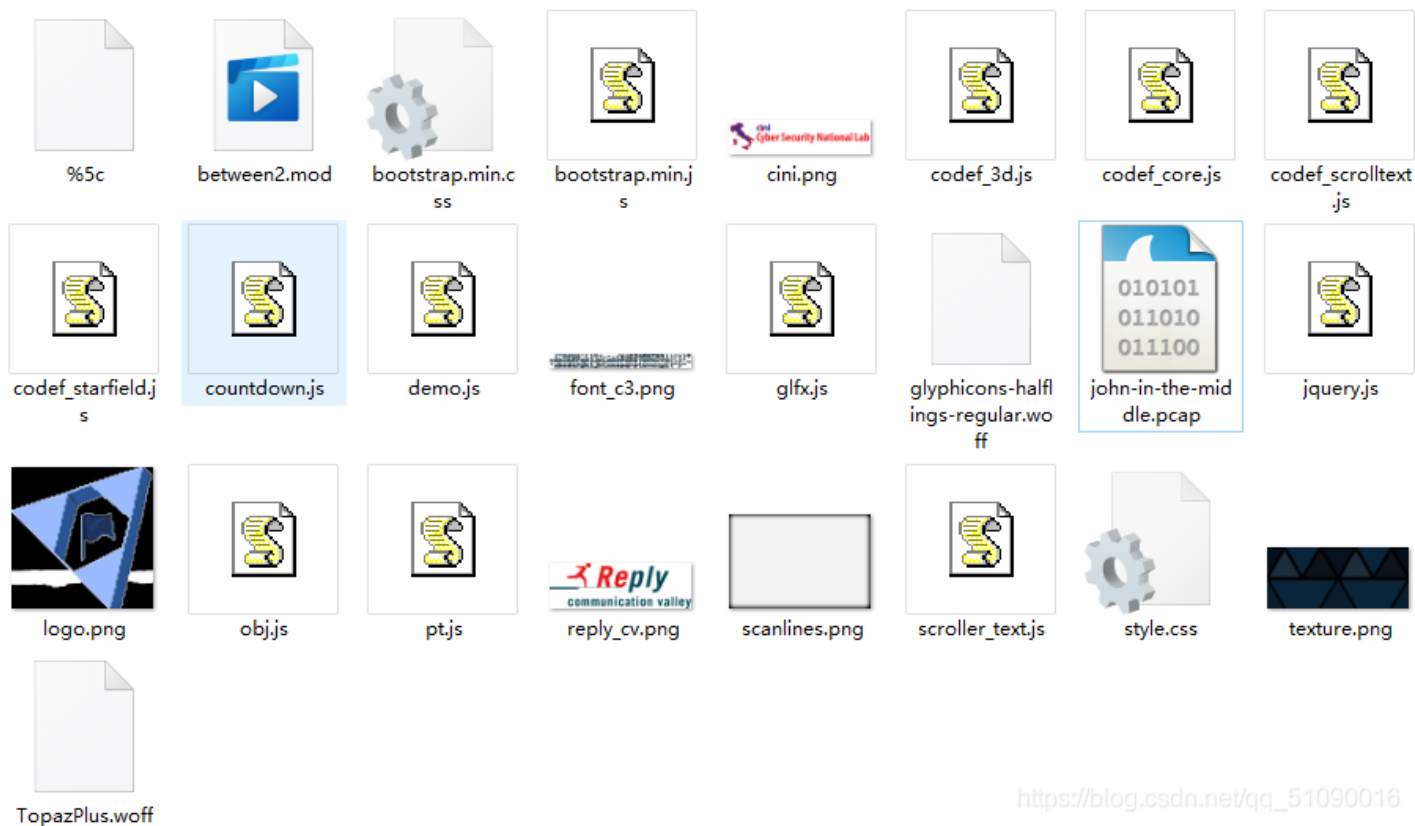
合起来：`wllmup_up_up`

使用这个密码解压flag2.zip，解压得到Real flag.jpg，使用010 Editor打开搜索关键词ctf即可得到flag

john-in-the-middle(导出 http)

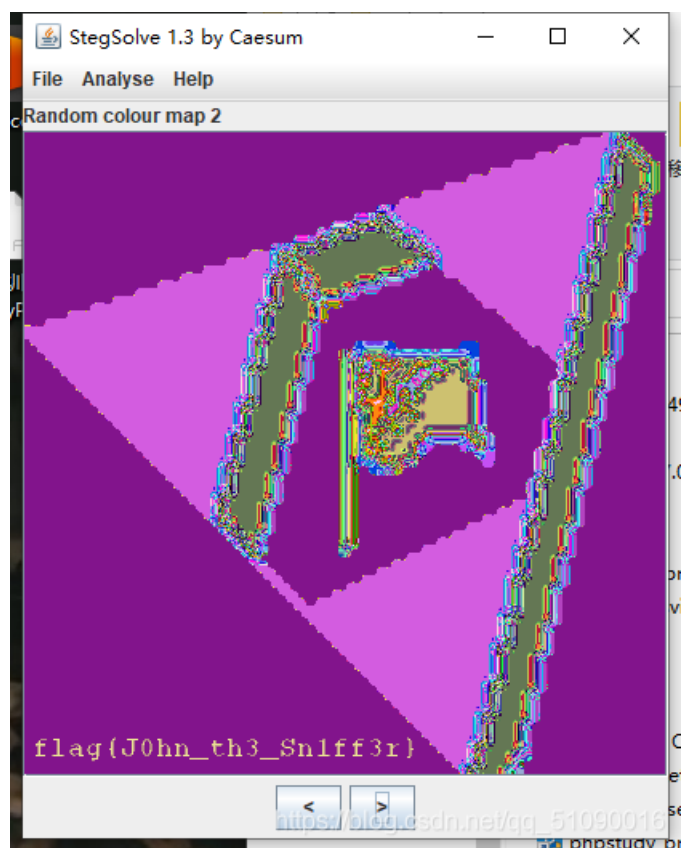
wireshark打开文件后，查看数据量并没有线索，然后我就麻了，看wp

需要导出http，具体步骤：文件 → 导出对象 → http → save all



https://blog.csdn.net/qq_51090016

得到了好多东西，从6张png下手，一个个在stegsolve中打开，终于在logo.png里面找到了（好狗）



低个头（键盘加密??）

MZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2G IYJVHA4TONZYGA2DMM3FGMYH2

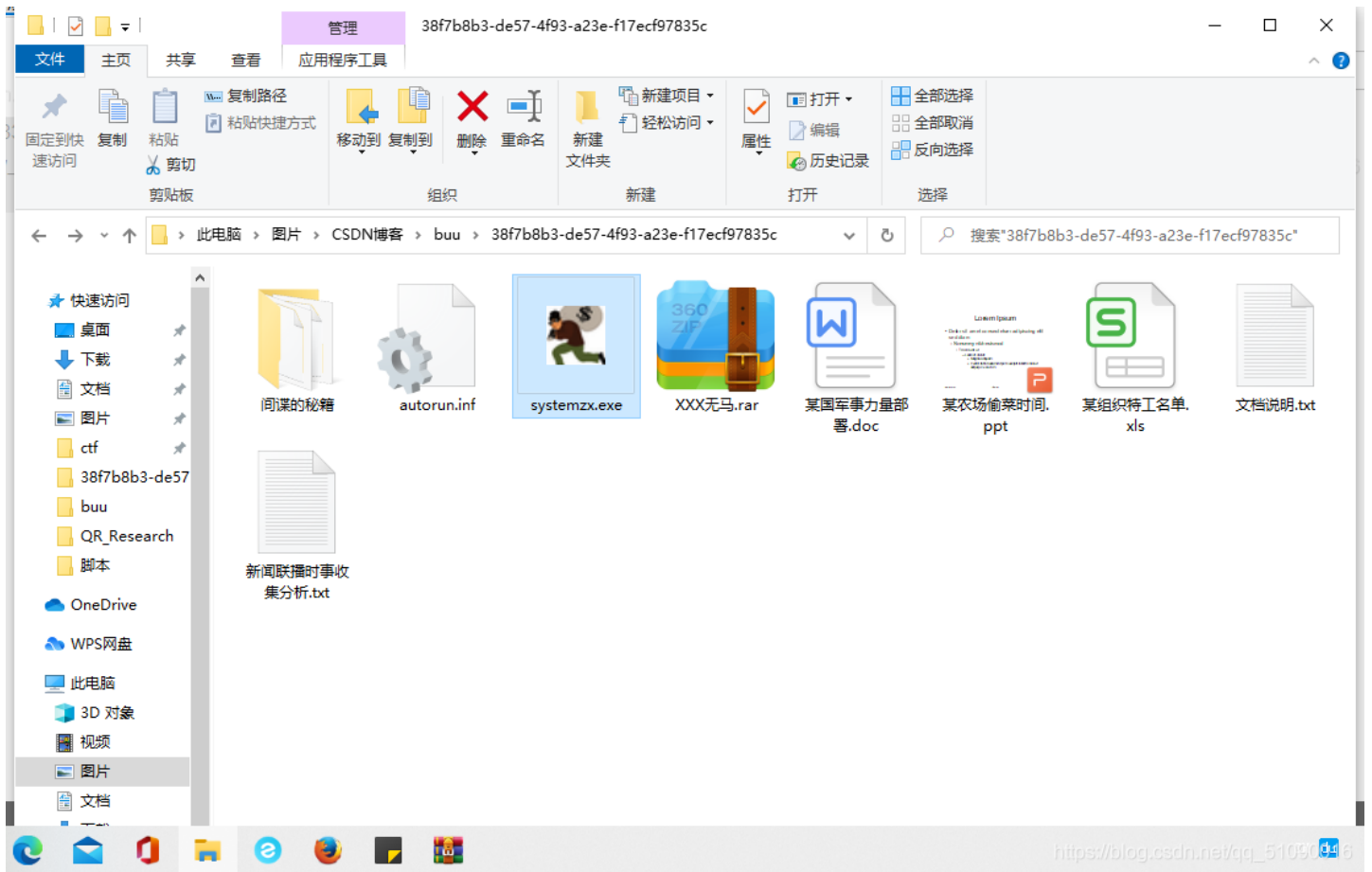
编码 解码 清空

flag{6f1797d4080b29b64da5897780463e30}

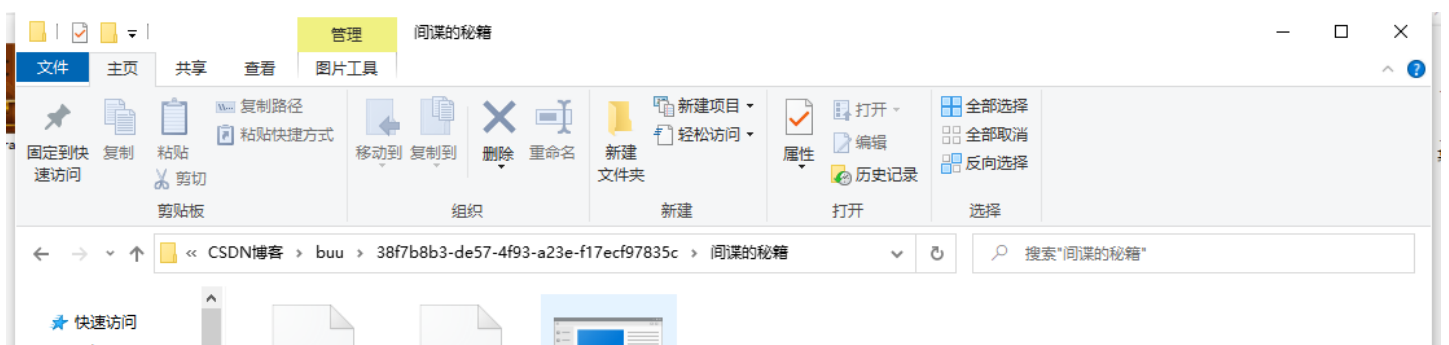
https://blog.csdn.net/qq_51090016

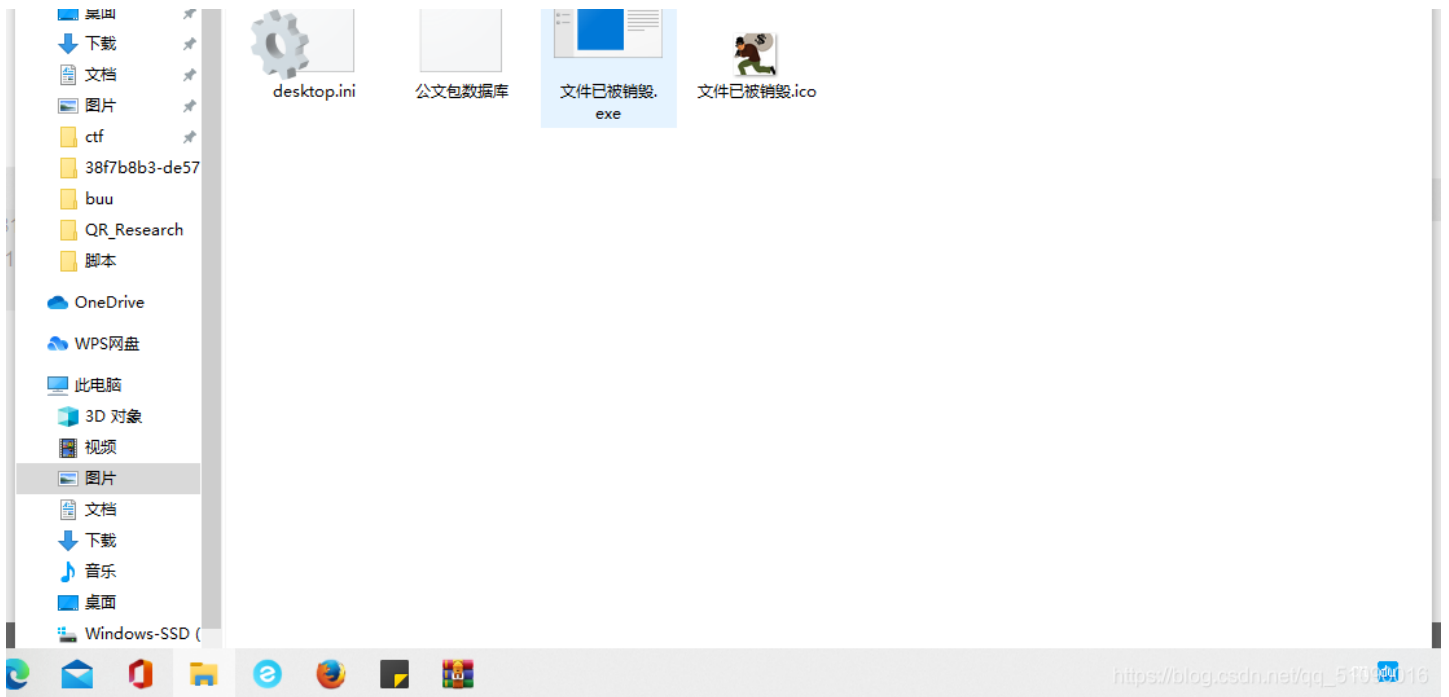
间谍启示录（奇怪的题目）

解压后看到一堆文件，只有这个exe有点东西



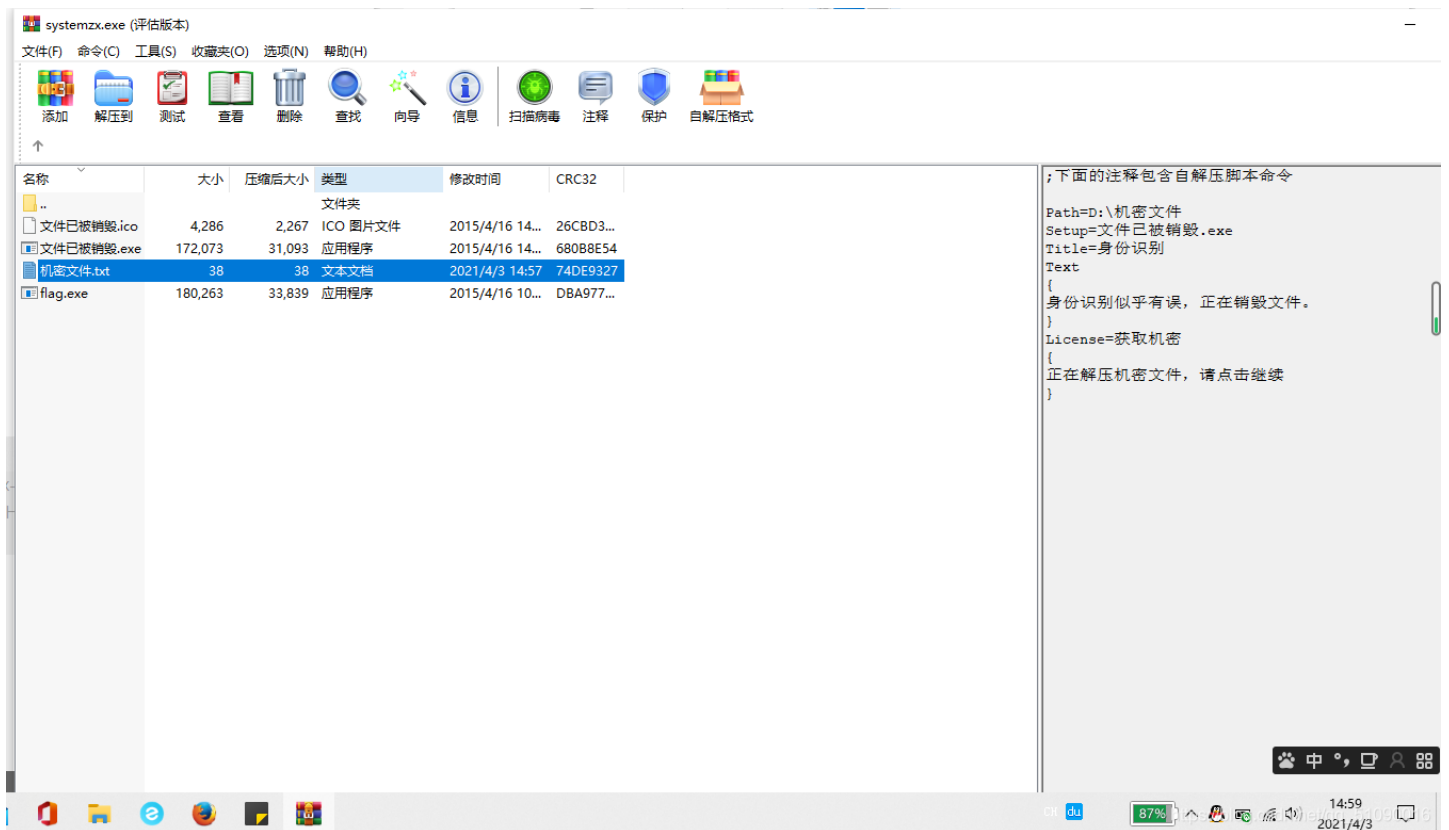
直接点开就被销毁了





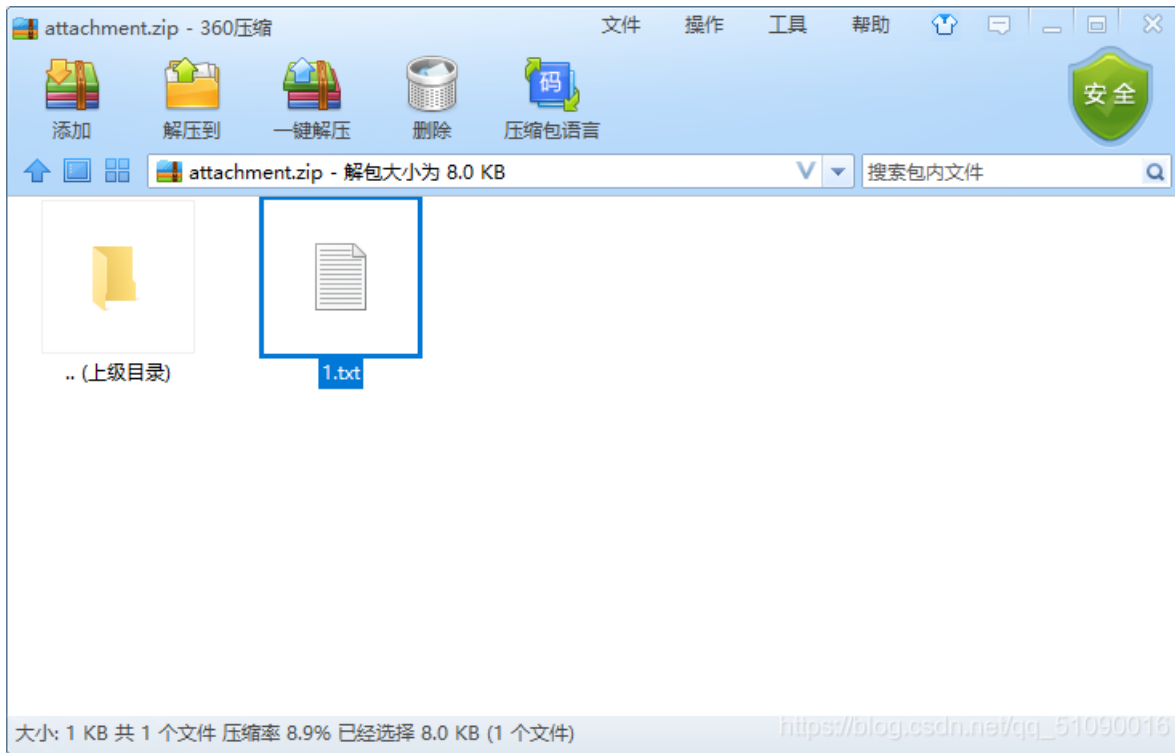
想到解压或者foremost也行

点那个flag.exe就会生成机密文件



[SUCTF2018]single dog(AAEncode解密)

用010打开发现里面有其他文件，改成zip后缀打开



里面是一大段表情。。。这就涉及到我的知识盲区了，百度吧

AAEncode加密/解密



```
function a()
{
  var a="SUCTF(happy double eleven)";
  alert("双十一快乐");
}
a();
```

淘宝搜索

https://blog.csdn.net/qq_51090016

[安洵杯 2019]吹着贝斯扫二维码

这题需要用到改后缀的脚本，但我运行一直出错啊啊啊啊啊啊。。。

从娃娃抓起（中文电码）

两个txt文件，第一个：

```
从娃娃抓起.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
0086 1562 2535 5174
bnhn s wwv vffg vffg rrhy fhv
```

请将你得到的这句话转为md5提交，md5统一为32位小写。
提交格式：flag{md5}

中文电码和五笔编码

```
0086 1562 2535 5174 中文电码
人 工 智 能
bnhn s wwv vffg vffg rrhy fhv 五笔编码
也 要 从 娃 娃 抓 起

请将你得到的这句话转为md5提交，md5统一为32位小写。
提交格式：flag{md5}
```

第二个是提示

```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
题目描述：伟人的一句话，标志着一个时代的开始。那句熟悉的话，改变了许多人的一生，为中国三十年来计算机产业发展铺垫了道路。两种不同的汉字编码分别代表了汉字信息
```

md5加密：

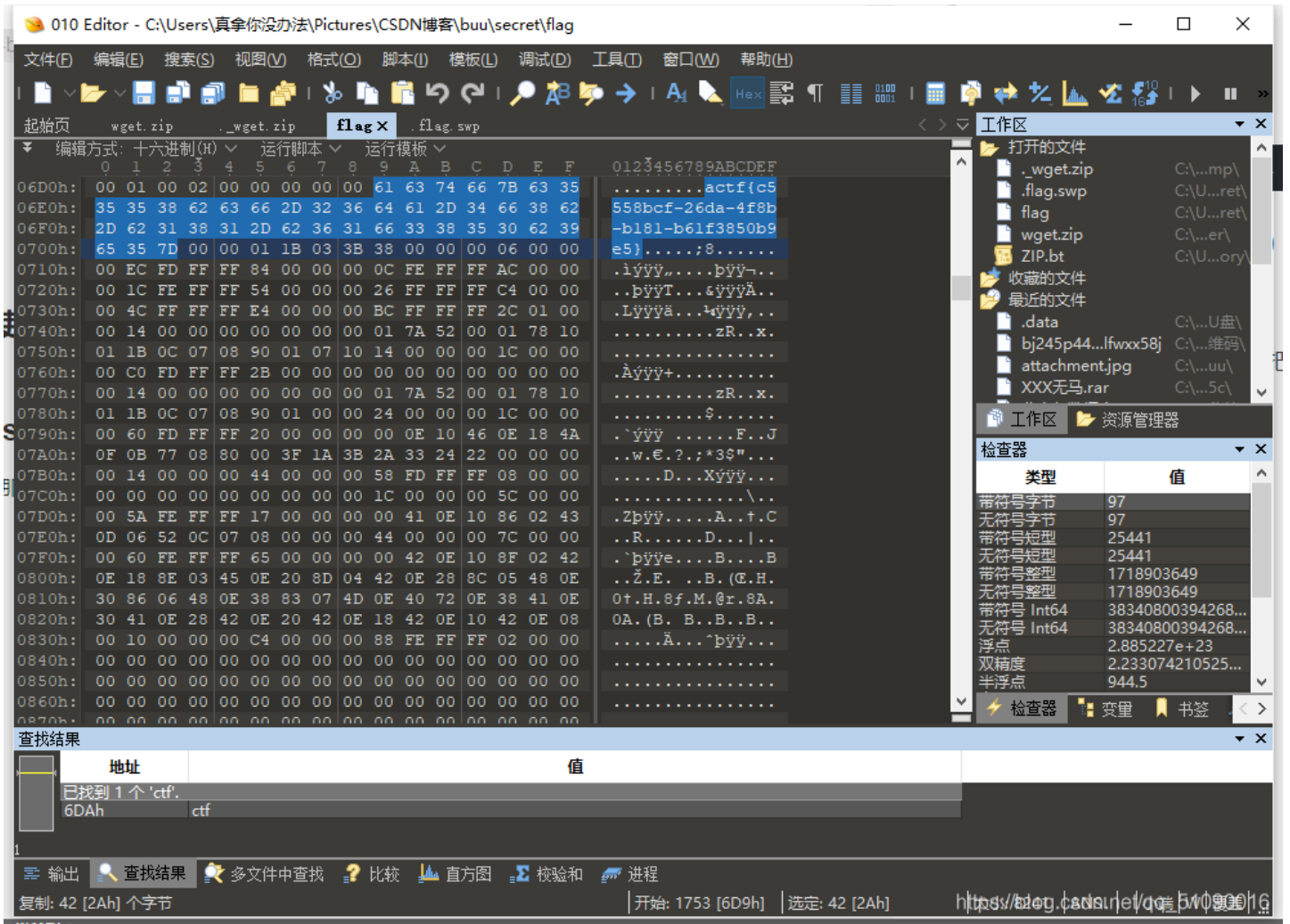
```
3b4b5dccd2c008fe7e2664bd1bc19292
```

小易的U盘（ida的使用）

这个本来ida一直出错。。百得知ida安装路径不能有中文，改了之后就好了

[ACTF新生赛2020]swp（导出http）

这题主要是根据swp的提示想到把那个pcapng文件导出http，获得了一堆文件，里面有一个压缩包，解压后搜索ctf就有了



百里挑一

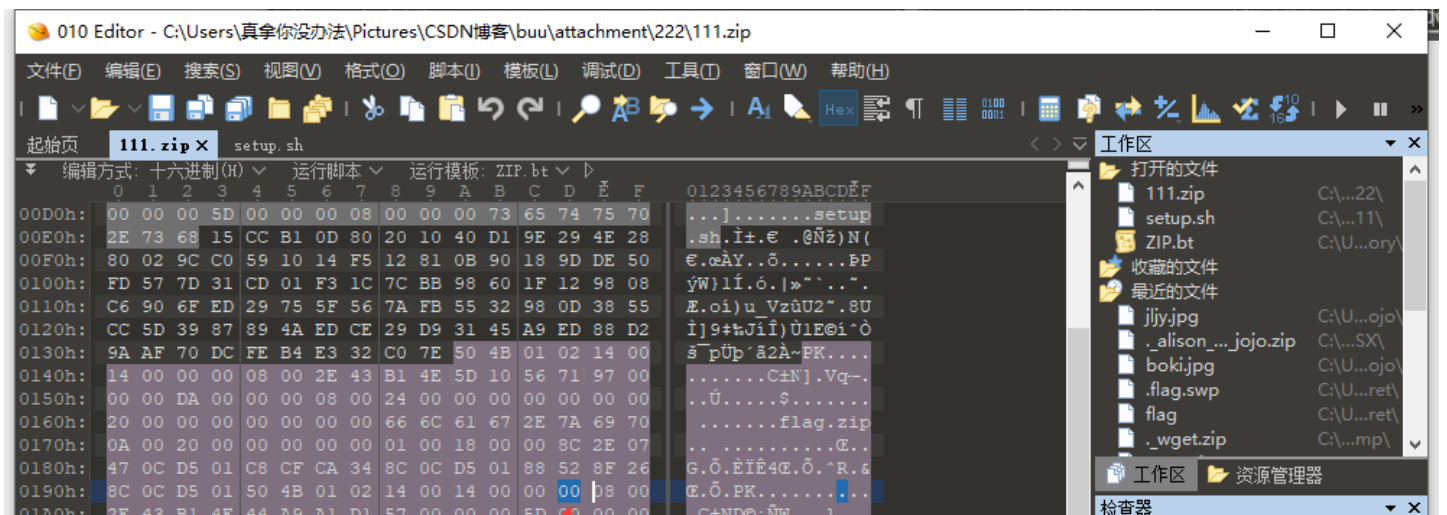
[WUSTCTF2020]alison_likes_jojo (outguess隐写)

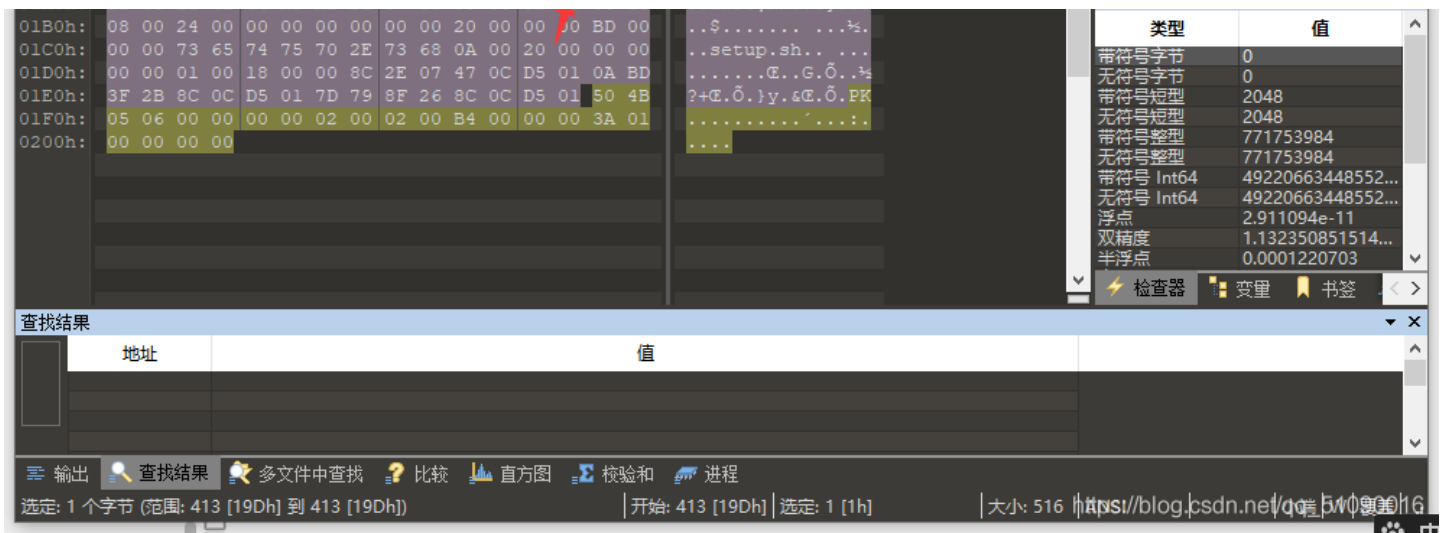
这一题只做了一半，outguess遇到的太少了，还是太菜了

[GUET-CTF2019]zips (伪加密 python时间戳?)

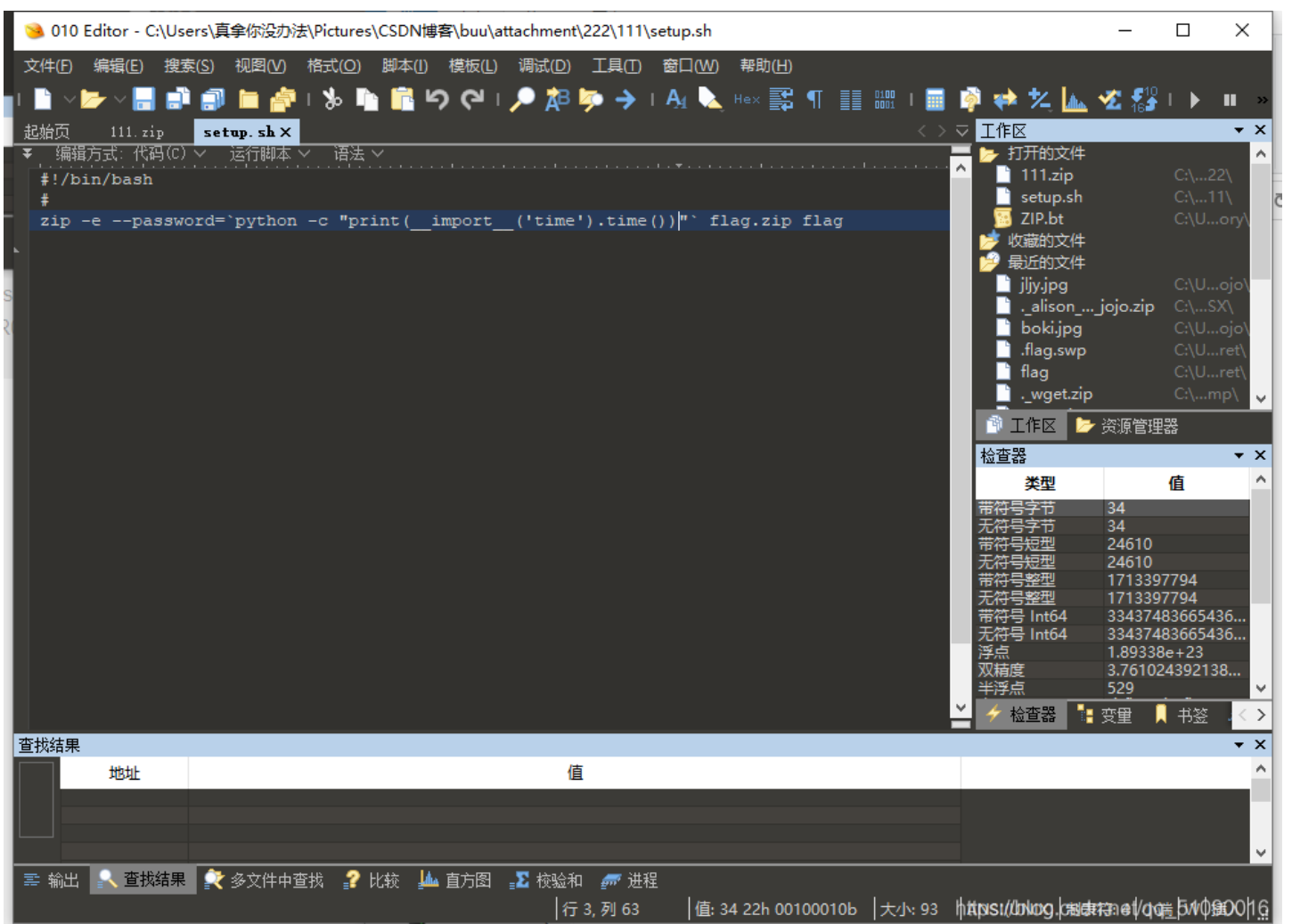
zip伪加密还是没搞透，先是第一层的爆破，得到密码723456

然后是第二层的伪加密：把这个位置的09改成00就行了





解压得到

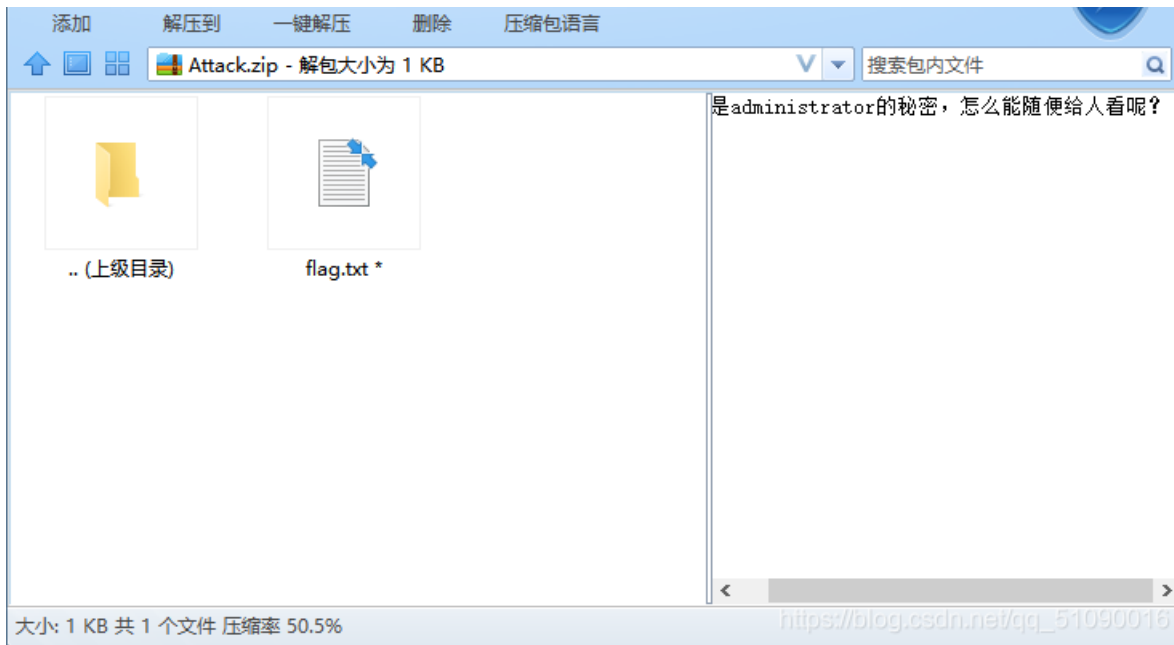


这是要执行这段代码么

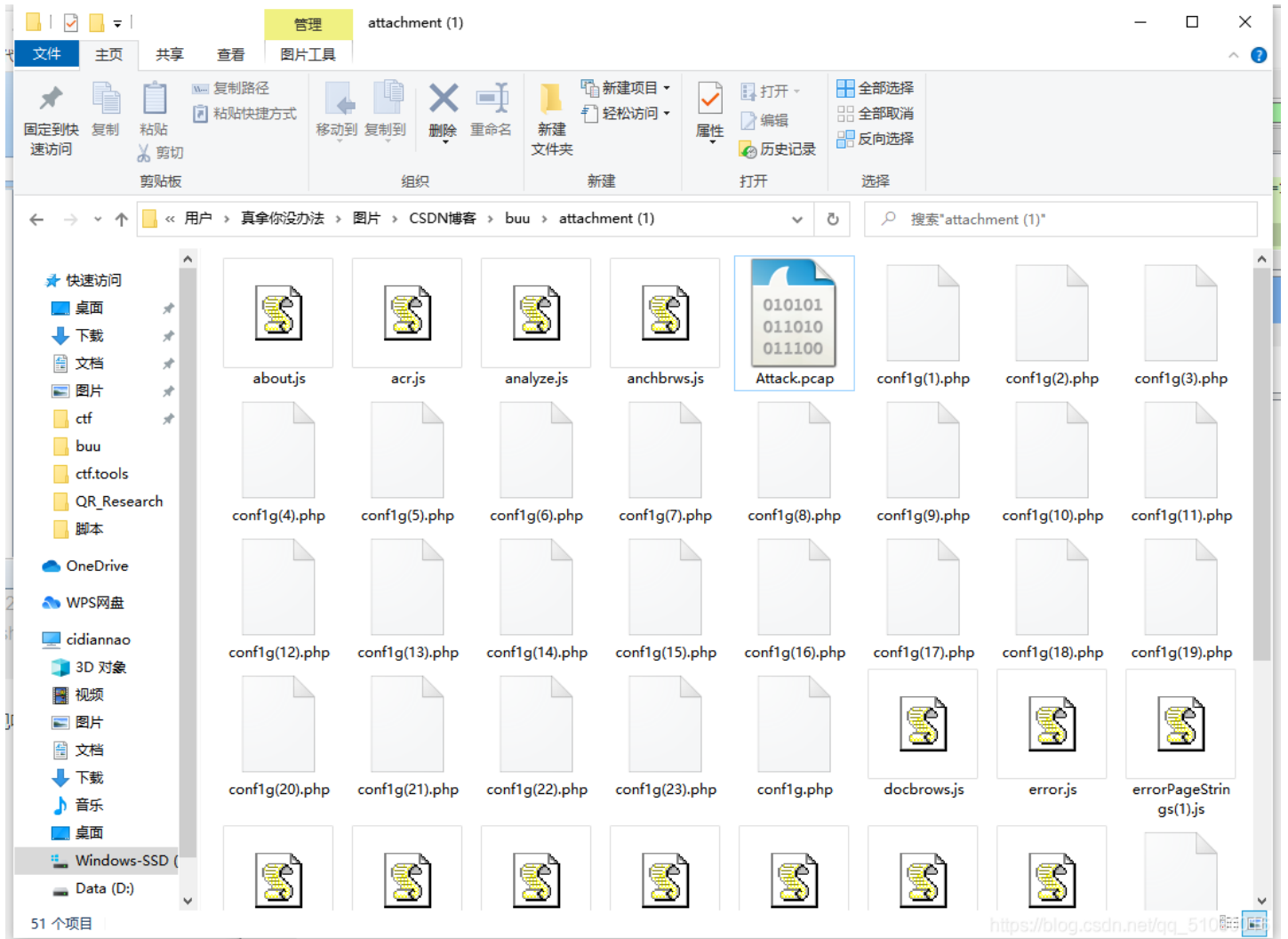
```
C:\Users\真拿你没办法\Pictures\CSDN博客\buu\attachment\222\111\setup.sh
1617716051.4345222
```

执行完了。。怎么不是密码,看 WP 吧

因为时间戳和出题当时不太一样所以往前推, 利用ARCHPR设置掩码15???.?? 掩码符号为***



密码肯定要在原文件里搞到了，我先是看tcp流。。真的没发现啥东西，再导出http



这一堆实在让我不知道干啥。。看wp吧

lsass.exe是一个系统重要进程，用于微软Windows系统的安全机制。它用于本地安全和登陆策略。

这里利用mimikatz获取明文密码，保存lsass下来放入mimikatz同目录下（64位）

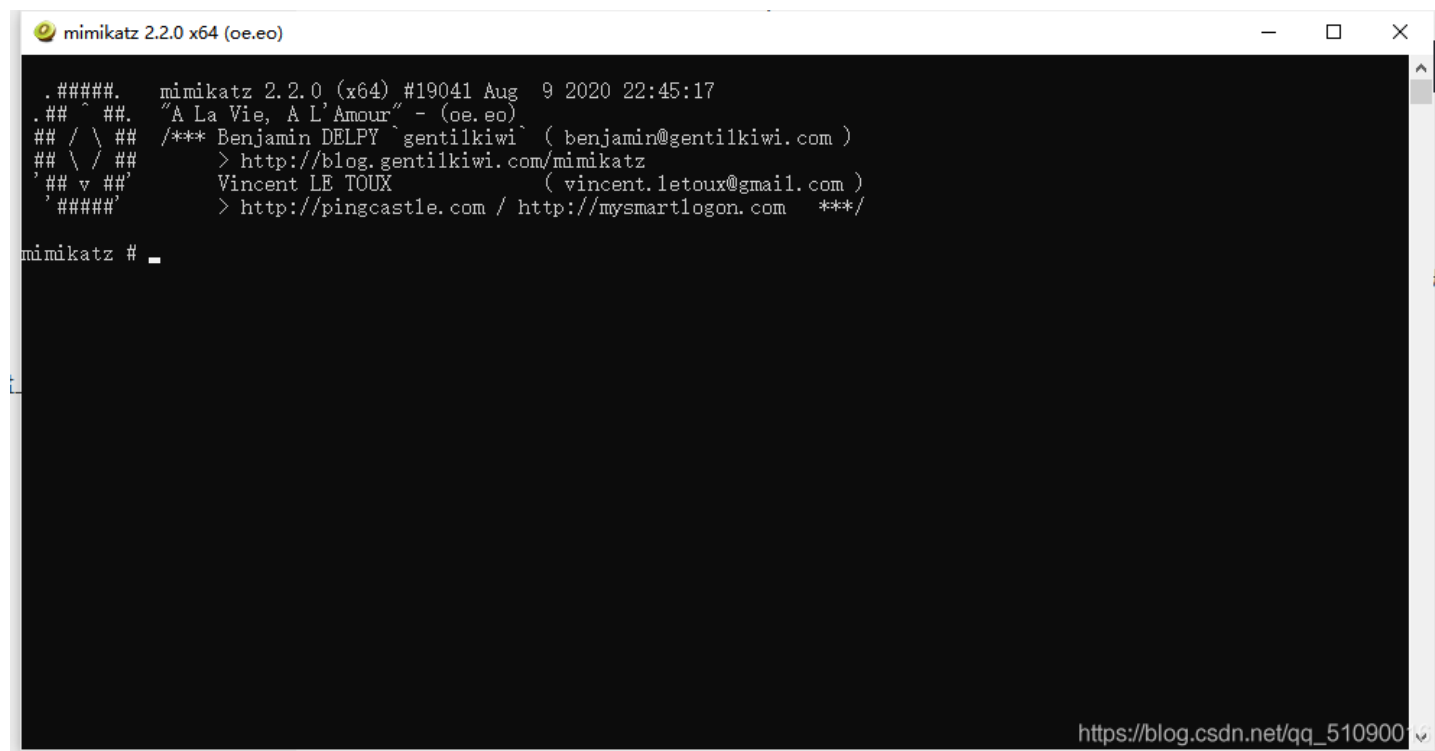
用x64位右键管理员运行打开

mimikatz（内网渗透工具，可在lsass.exe进程中获取windows的账号明文密码）

这里的minikatz我在github上下载没有exe文件。。。可能是被直接删掉了，最后从下面这个大佬的网盘上下的

https://blog.csdn.net/weixin_45663905/article/details/108013149

用管理员权限才能打开：



```
#####. mimikatz 2.2.0 (x64) #19041 Aug 9 2020 22:45:17
.## ^ ##. "A La Vie, A L'Amour" - (oe.oe)
## / \ ## /*** Benjamin DELPY`gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # _
```

具体步骤：

```
//提升权限
privilege::debug
//载入dmp文件
sekurlsa::minidump lsass.dmp
//读取登陆密码
sekurlsa::logonpasswords full
```

搜索一下password



```
wdigest :
* Username : Administrator
* Domain   : WIN7
* Password : W31c0meToD0g3
kerberos :
* Username : Administrator
```

有了
输入密码解压就行了

[SUCTF 2019]Game

先是用vs code打开发现一串base32

```
</div>
<div class="text text--best-time">
  <icon trophy></icon>
  <span>Well done!,
  <?php echo "here is your flag:|ON2WG5DGPNUECSDBNBQV6RTBNMZV6RRRMFTX2=== " ?>
  </span>
</div>
```

得到 `suctf{hAHaha_Fak3_F1ag}`

假的flag。。。

再看另一张图片，LSB发现一串base64

这串base64解码后头部是Salted，应该是AES或者3DES



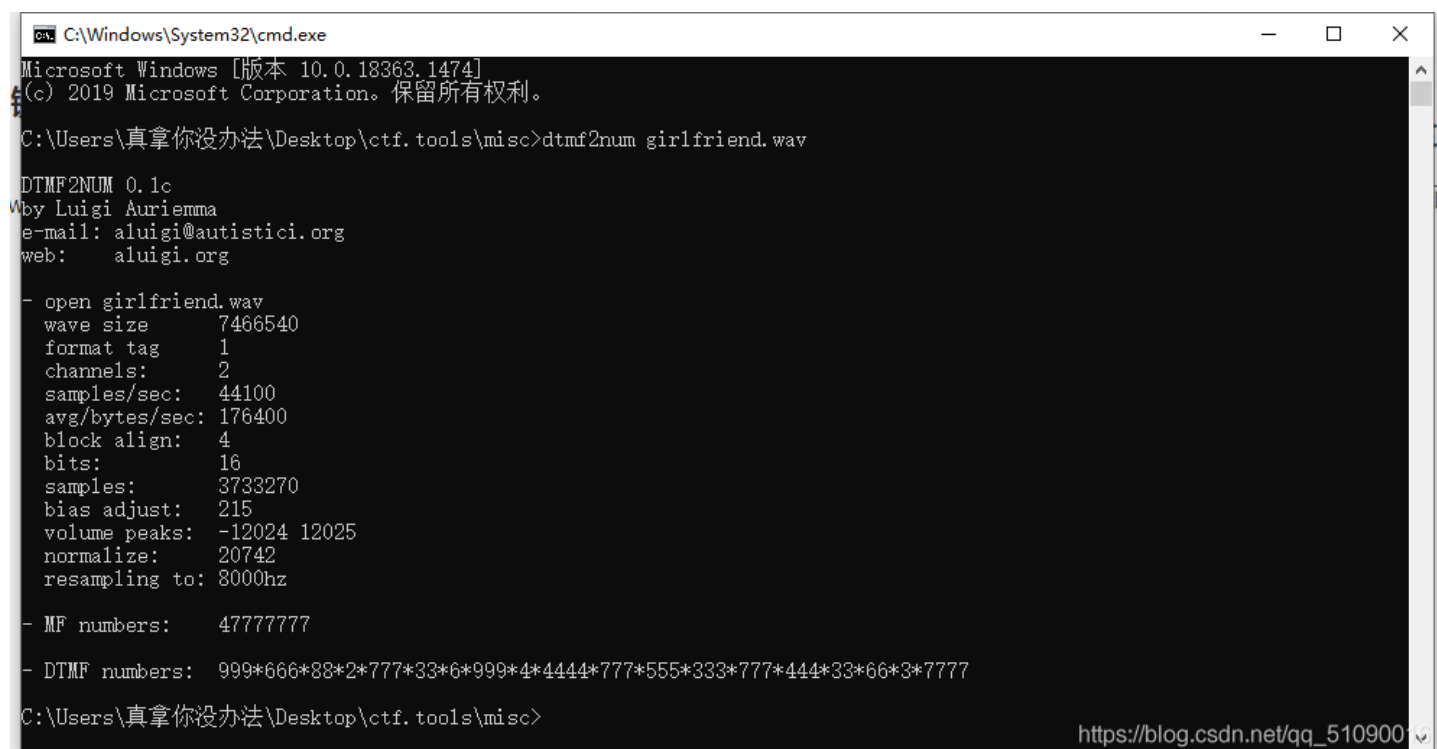
[WUSTCTF2020]girlfriend (DTMF拨号音 手机键盘密码)

先是将音频用audacity打开，结果并不是摩斯电码，麻了，不知道啥东西，看wp

猜测DTMF拨号音识别，有个程序可以识别一下dtmf2num.exe

下载地址

放在同一个文件夹下打开cmd



然后就是手机键盘密码



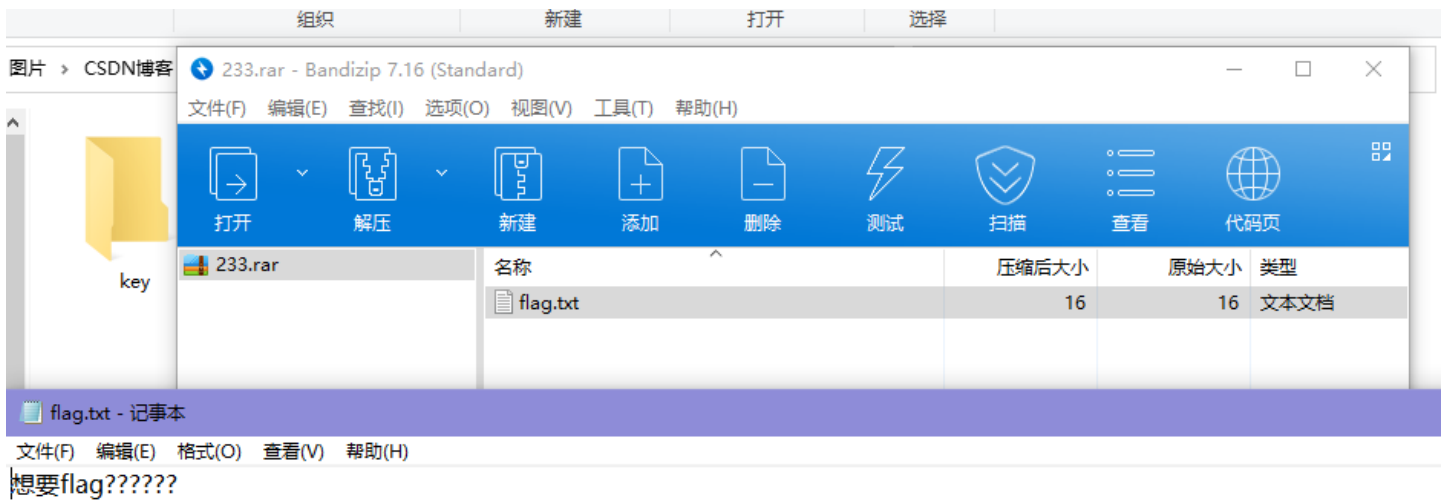
```
999 ---> y  
666 ---> o  
88 ---> u  
2 ---> a  
777 ---> r  
33 ---> e  
6 ---> m  
999 ---> y  
4 ---> g  
4444 ---> i  
777 ---> r  
555 ---> l  
333 ---> f  
777 ---> r  
444 ---> i  
33 ---> e  
66 ---> n  
3 ---> d  
7777 ---> s
```

youaremygirlfriends

[MRCTF2020]CyberPunk

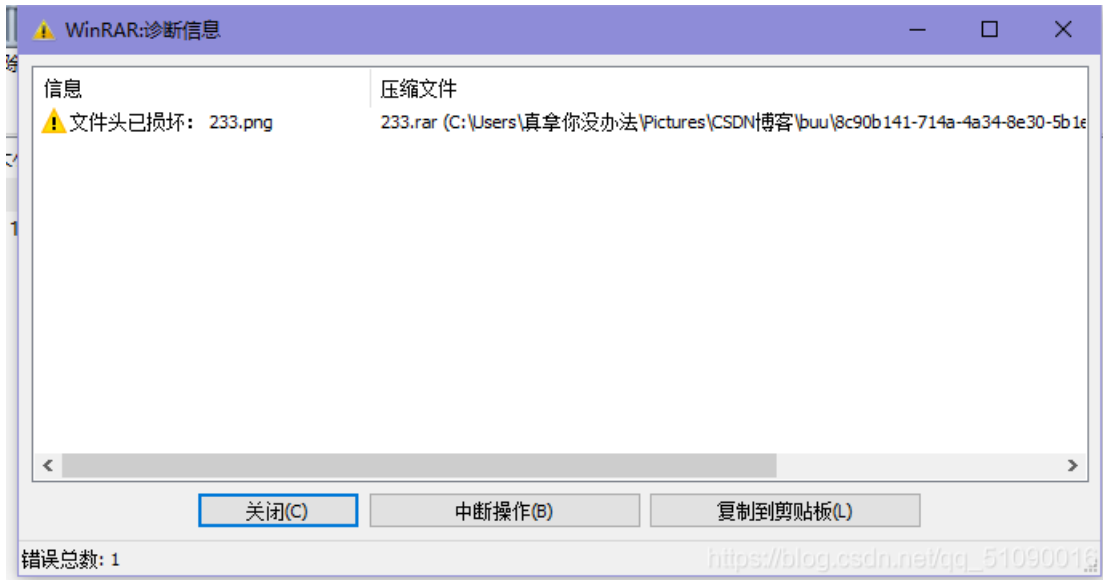
又是一道脑洞题

再回过头看另一个rar文件，里面的txt文件显然并没有flag



https://blog.csdn.net/qq_51090016

用WinRAR打开显示文件头损坏



https://blog.csdn.net/qq_51090016

010打开看看

The screenshot shows the 010 Editor interface with a RAR file open. The main window displays the file's header in hexadecimal and ASCII. A yellow error bar at the bottom indicates a "Header CRC mismatch in Block #3" at position 0x000010b, with a value of 8252h. The status bar also shows the file path and a URL.

010 Editor - C:\Users\真拿你没办法\Pictures\CSDN博客\buu\8c90b141-714a-4a34-8e30-5b1ecbcf328b\233.rar

文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 脚本(I) 模板(L) 调试(D) 工具(T) 窗口(W) 帮助(H)

起始页 233.rar x

编辑方式: 十六进制(H) 运行脚本 运行模板: RAR.bt

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF

```
0000h: 13 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 Rar!...i.s.....
0010h: 00 00 00 00 D7 62 7A A0 90 2C 00 38 B0 18 00 F4 ....<bz,,.8°.ô
0020h: FC 19 00 02 E9 79 8D 9C 16 7A 25 4C 1D 33 07 00 ü...éy.æ.zL.3..
0030h: 20 00 00 00 32 33 33 2E 70 6E 67 00 B0 DF 83 4D ...233.png^°AfM
0040h: 11 D9 99 94 C8 95 DD 94 11 5D A0 25 88 59 48 88 .Û""È·Ý" ] %*YH*
0050h: A4 2C 28 0A 59 88 25 96 1B 03 32 25 88 58 52 2A H, (.Y~%-..2%XR*
0060h: 6C 02 6C 8A 84 05 12 D3 08 5F 50 20 22 20 20 25 1.1š,,.ó._P " %
0070h: F4 05 04 04 04 B6 88 96 A0 11 41 2D A5 FD 56 B5 ó...¶^-.A~¥ýVu
0080h: E7 DF 1C FD CA 0E 33 FB 5E 7F 3A AD 7A 14 AA 28 çß.ýË.3û^.-z.ª.(
0090h: AA 84 25 63 18 EF AE FA EB 9E 78 E7 B3 D2 BD 6C ª,,%c.i@úéžxcªÖ±l
00A0h: 25 7C E3 8F 47 44 76 D6 54 CB 0A 4C 8A 41 7E 82 %|ã.GDvÖTÈ.LšA~,
00B0h: C5 55 45 11 5F DD CC AA FF 7E C1 91 81 E8 BD 93 ÅUE. Ýi*y-Å`.è±"
00C0h: 1C 77 7F E0 D8 12 AA 8A 87 75 F0 88 (6D) 9E B3 9B .w.àØ.ªš±uš"mžªª
00D0h: 9A E4 11 B6 E6 A3 FF 0E F3 CC E5 F3 60 74 F0 84 ša.qæÿ.ó!ãö`tš,,
00E0h: 8A 11 DD 40 DE 49 B6 C5 E9 16 9C 59 14 4A 9B 7E Š.Ý@B!qÅé.œY.J>~
00F0h: C6 B2 3C CE 2A AE 67 C7 39 DA 49 C2 9A 58 4B 12 Eª<î*øgç9úIãšXK.
0100h: C0 ED 73 06 26 2D 3F 16 FB 36 8A 2B CC 84 B7 E3 Å!s.c-?.ú6š+î,,-ã
0110h: 09 C7 49 C9 A7 A4 D6 D4 86 CE FF 6D 52 7C AC 1F .ÇIÉš#ÖÖ+îÿmR|~.
0120h: B3 DC 2F EC C2 1B 03 45 32 8B 52 E4 43 91 5D 9D ªÛ/iÅ..E2<RaC`].
0130h: 1D B9 1B EC 16 17 1C 2C F6 E4 C9 A2 D9 55 12 8E .ª.ì...øãÈ°ÛU.ž
0140h: 06 A3 88 02 C0 6C CF 8A 41 8A 38 CD 07 02 37 DC .È°.Å!šAš8í..7Û
0150h: E8 0B 41 E0 32 11 AA F2 78 4B 65 36 DA BA 1A AF è.Aà2.ªðxKe6Û°.
0160h: CC 34 90 17 F8 49 7D 51 D8 21 E2 82 48 8A CF 48 i4..øI|Qø!â,HšIH
0170h: 92 15 DF 8A 44 8B 2F 11 DB 12 88 58 61 0D DD 13 ' .BšD</.Û.ªXa.Ý.
0180h: FF 6F 3A D0 4D C4 BA B0 28 E1 5A 09 28 45 9D 63 ýo:DMÅ°° (ãZ. (E.c
0190h: 97 4B CF 29 31 44 4A 9B 36 56 FA 69 B4 9C D3 98 -KÍ) 1DJ>6Vú!ªÖ"
01A0h: 92 42 D3 54 DD CC D8 FF D3 24 0E CC 86 FF FB 54 ªBÓTýîøøø.î+;ãT
```

查找结果

地址	值

输出 查找结果 多文件中查找 比较 直方图 校验和 进程

Header CRC mismatch in Block #3 Pos: 0 [0h] 值: 82 52h 01010010b <https://bbs.csdn.net/q/qa/54000016>

crc错误，而且里面有个png图片，修复一下将70A0改为74A0

再用stegsolve打开图片，在一个通道里发现了二维码



得到 `ci{v3erf_0tygidv2_fc0}`

维吉尼亚解密

```
ci {v3erf_0tygidv2_fc0}
```

密钥 XINAN

```
fa{i3eei_0llgvgn2_sc0}
```

https://blog.csdn.net/qq_51090016

前面没有flag，但整个字符串里可以拼到，应该是栅栏密码，再进行栅栏解密

```
fa{i3eei_011gvgn2_sc0}
```

每组字数

```
flag(vig3ne2e_is_c00l)
```

https://blog.csdn.net/qq_51090016