BUUCTF-杂项-1

原创

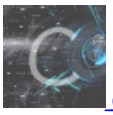
eeknight 于 2020-09-12 22:05:48 发布 889 收藏 1

分类专栏： ctf 杂项 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_46383107/article/details/108555800

版权


ctf 同时被 3 个专栏收录

1 篇文章 0 订阅

订阅专栏


杂项

1 篇文章 0 订阅

订阅专栏


BUUCTF

1 篇文章 0 订阅

订阅专栏

BUUCTF

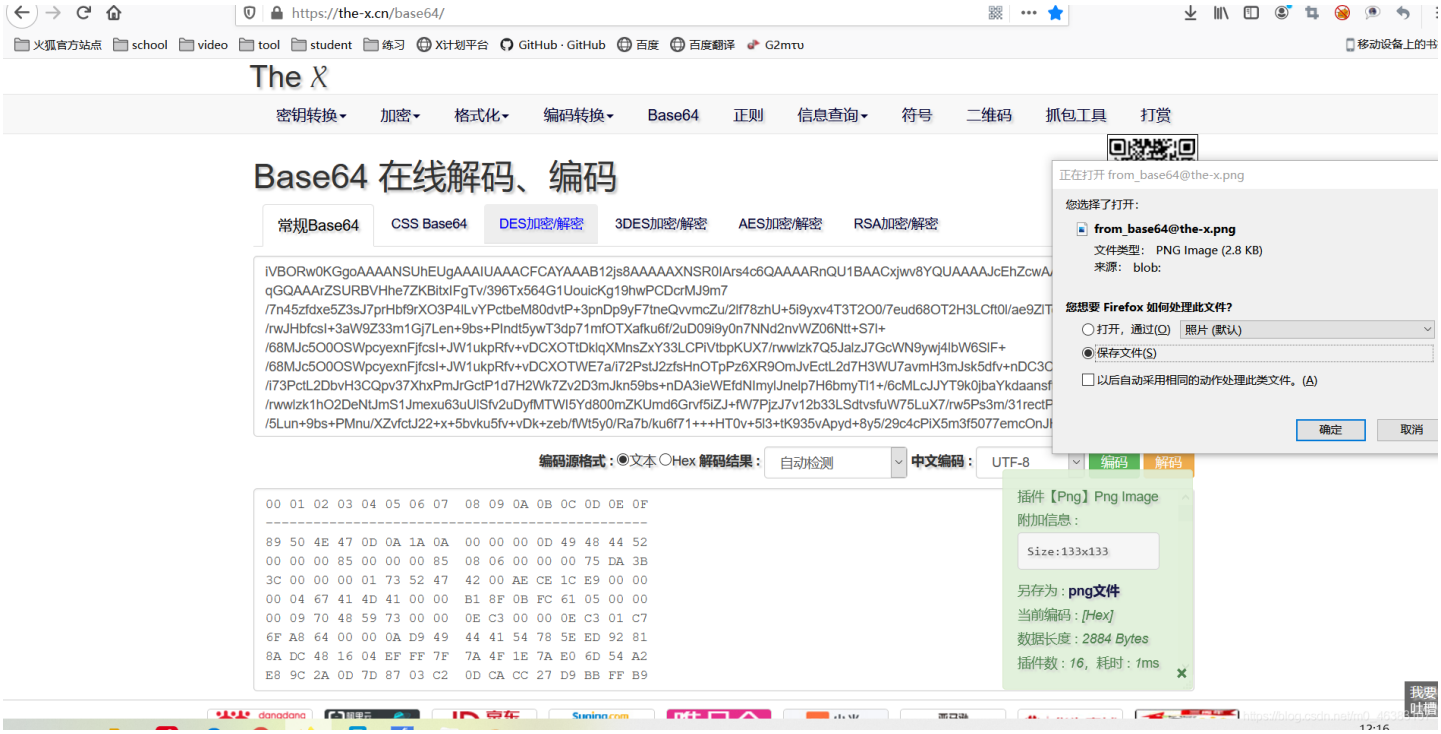
杂项

文章目录

N种方法解决

打开后下载文件key.exe

放到010Editor.exe里面可以看到一段文本



由于前面是image/jpg 和base64加密 就直接去网上解密并弄成图片形式

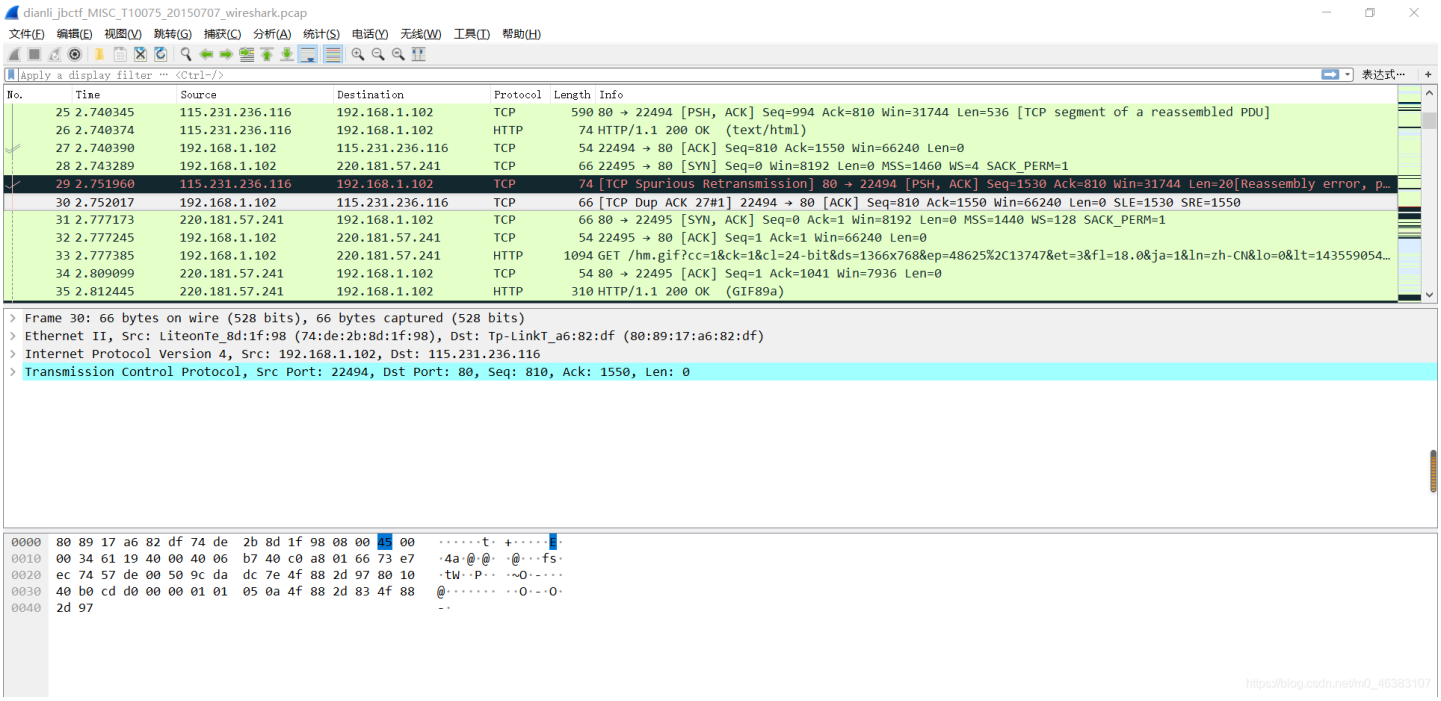
网站：https://the-x.cn/base64/（注意要把前面的这一段去掉才可以编译）

得到一个二维码 扫完就有flag

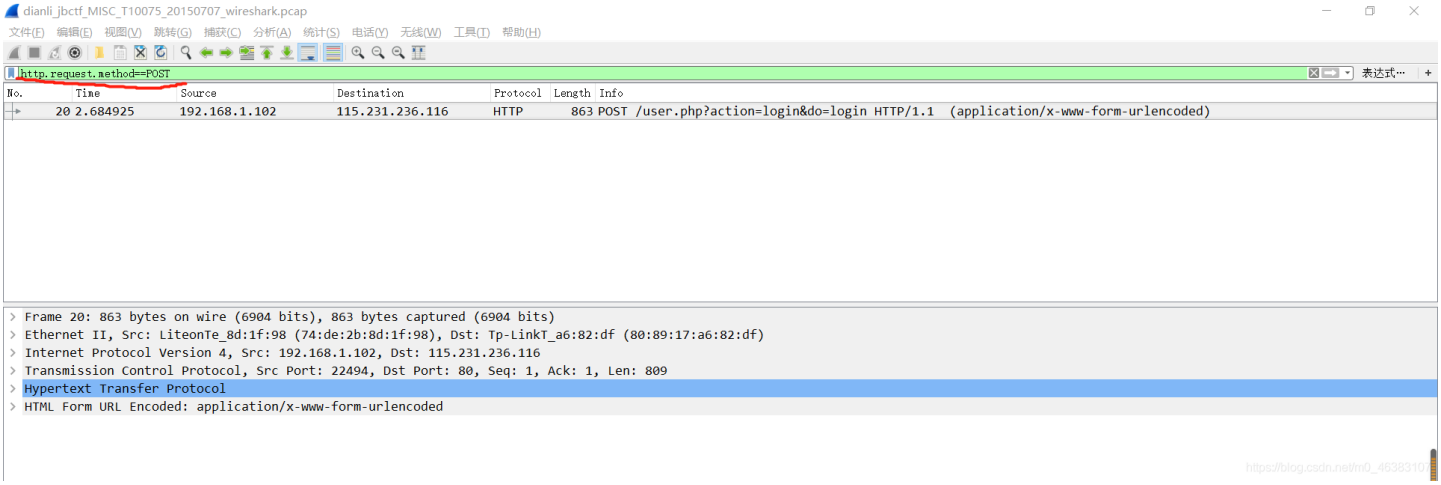
wireshark

这里要用到wireshark这个工具–虚拟机上有

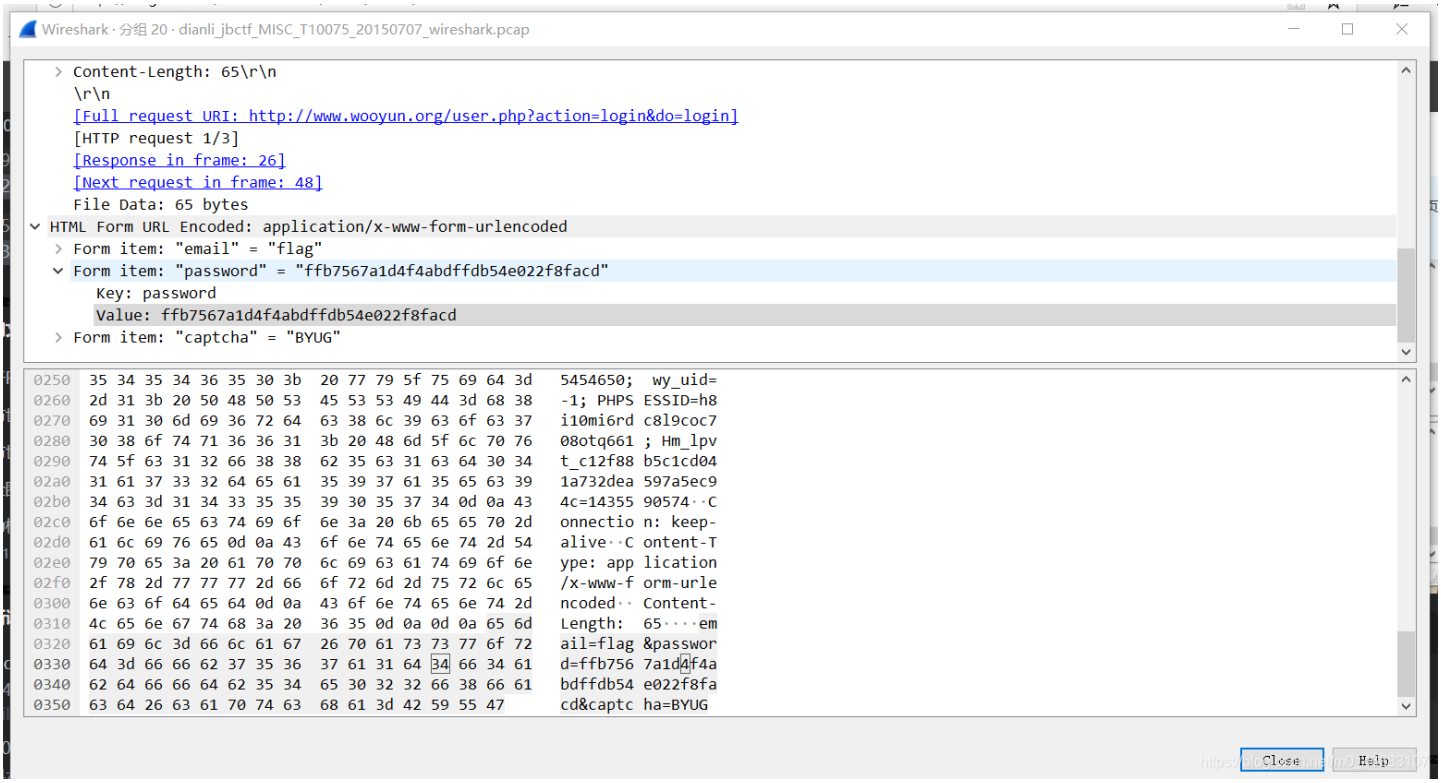
下载后打开看到一堆东西



根据提示直接过滤出POST包（好像flag一般在POST这里）



找到flag–value里面的数据就是flag

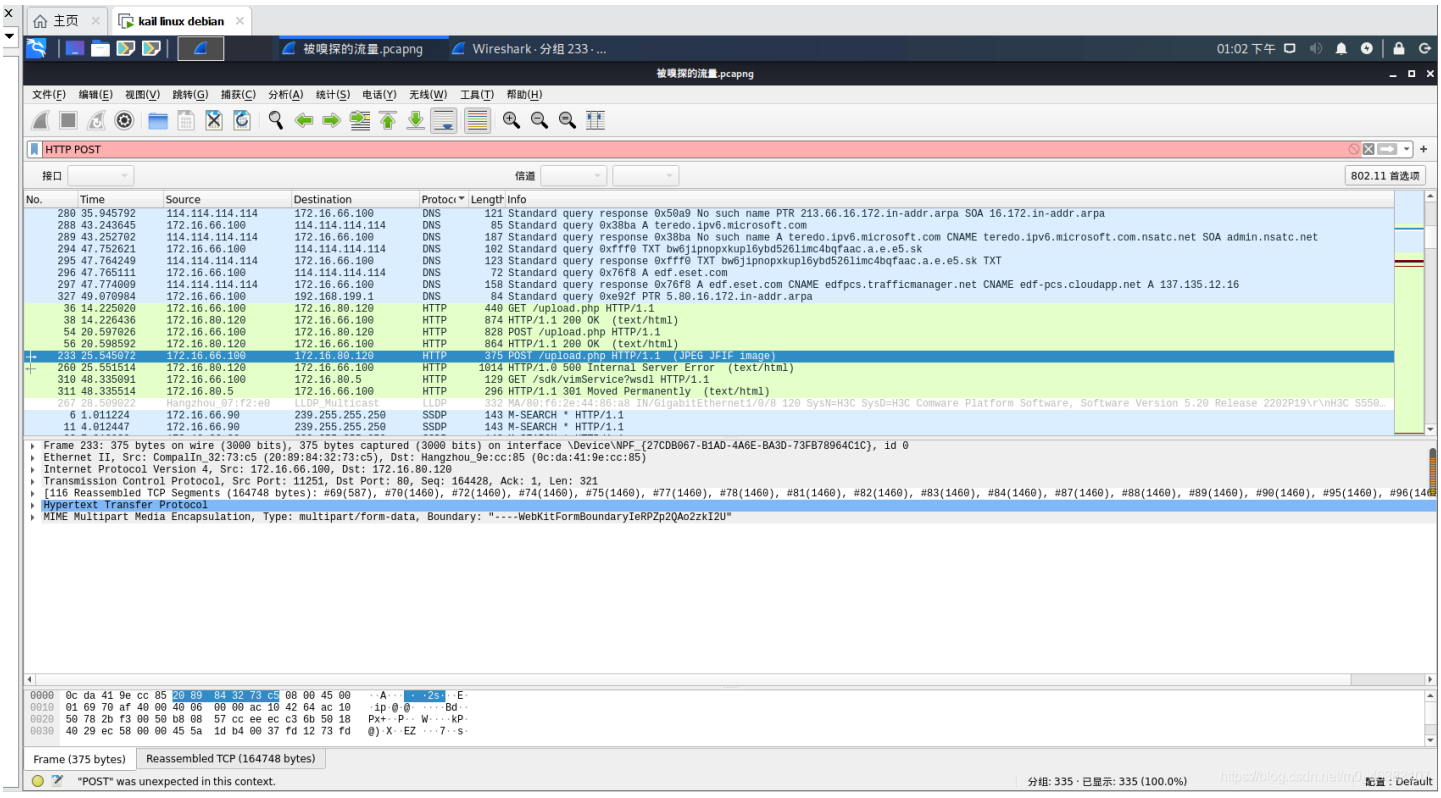


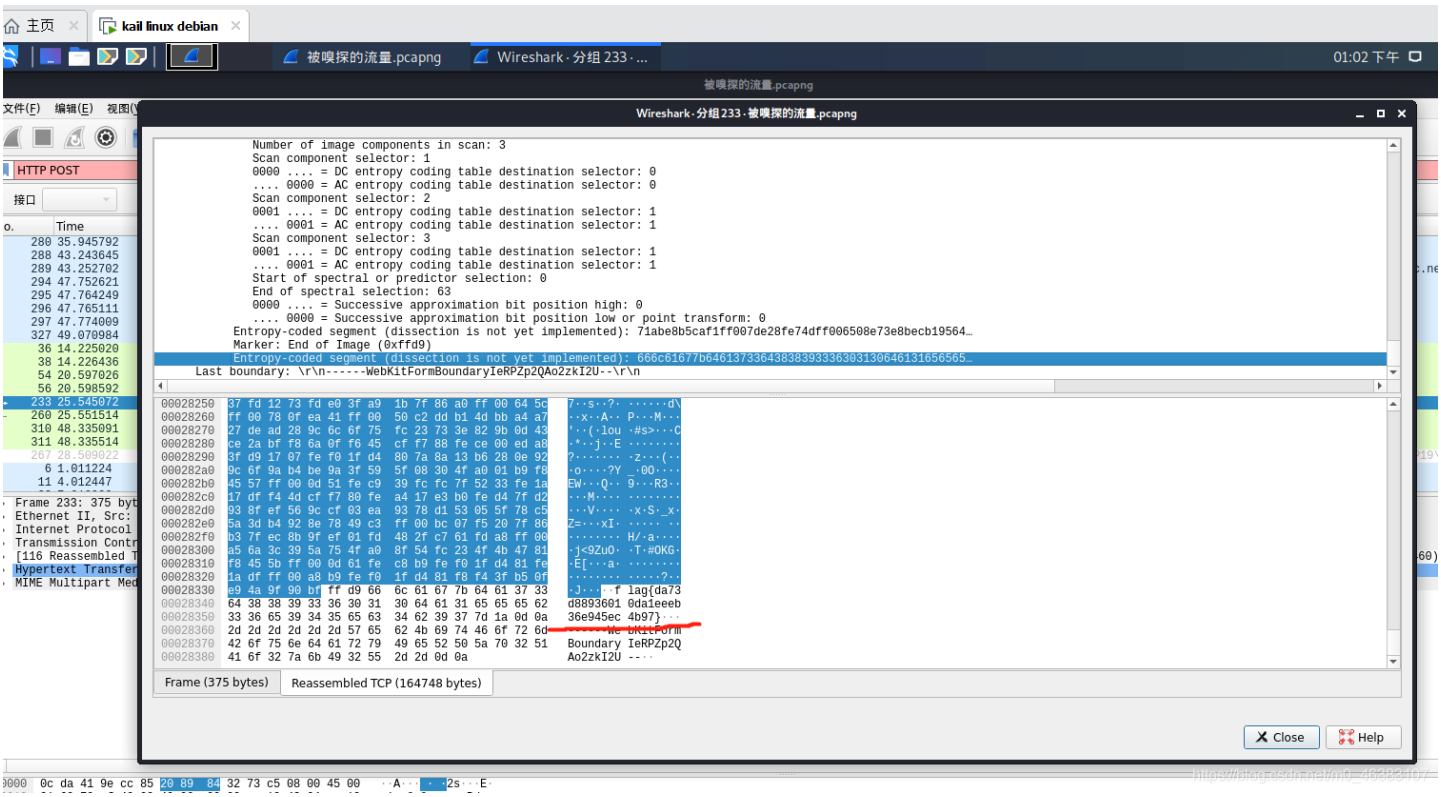
被嗅探的流量

某黑客潜入到某公司内网通过嗅探抓取了一段文件传输的数据，该数据也被该公司截获，你能帮该公司分析他抓取的到底是什么文件的数据吗？ 注意：得到的 flag 请包上 flag{} 提交

下载文件

用wireshark看

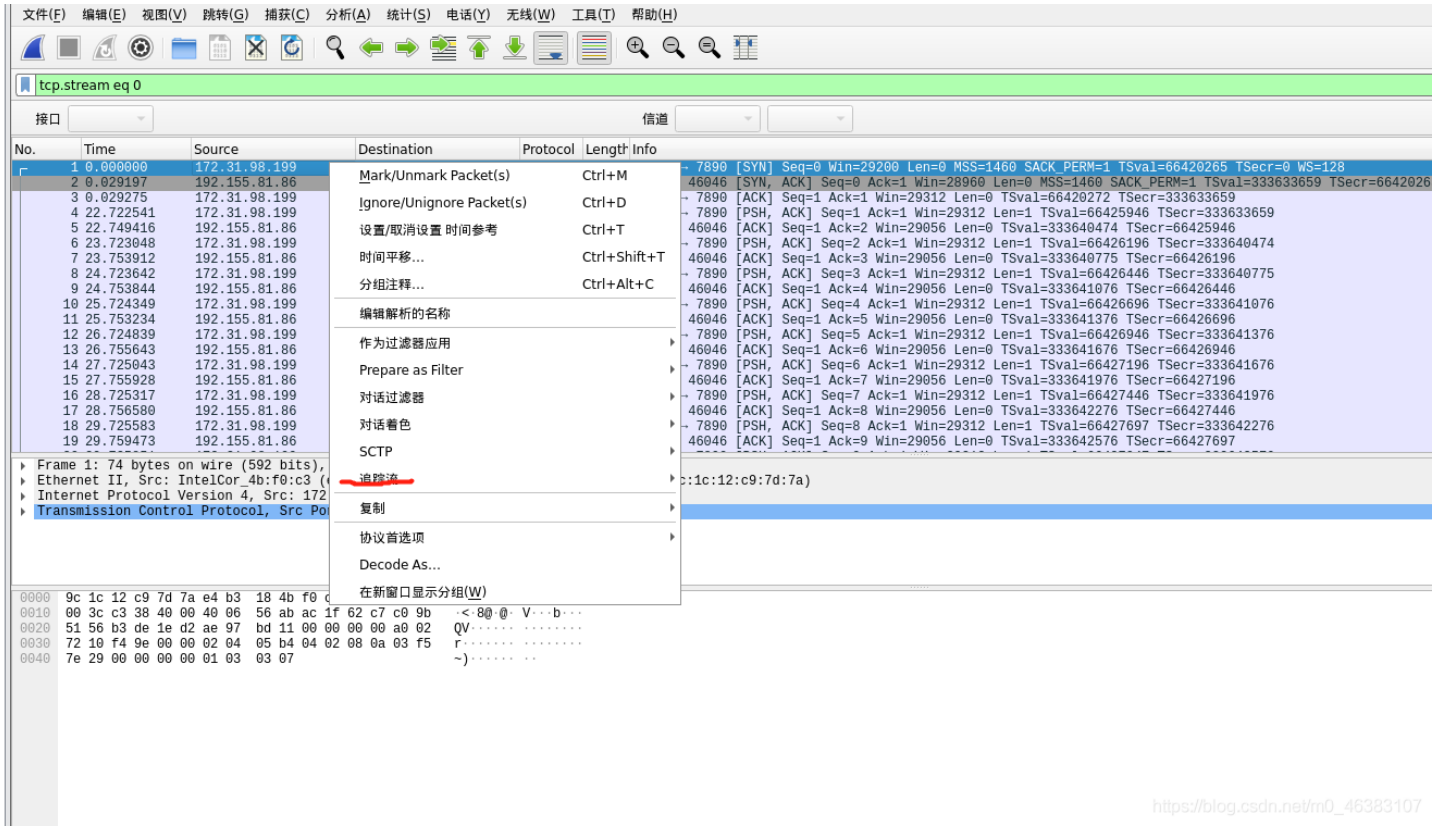




easycap

下载后直接丢到wireshark里面

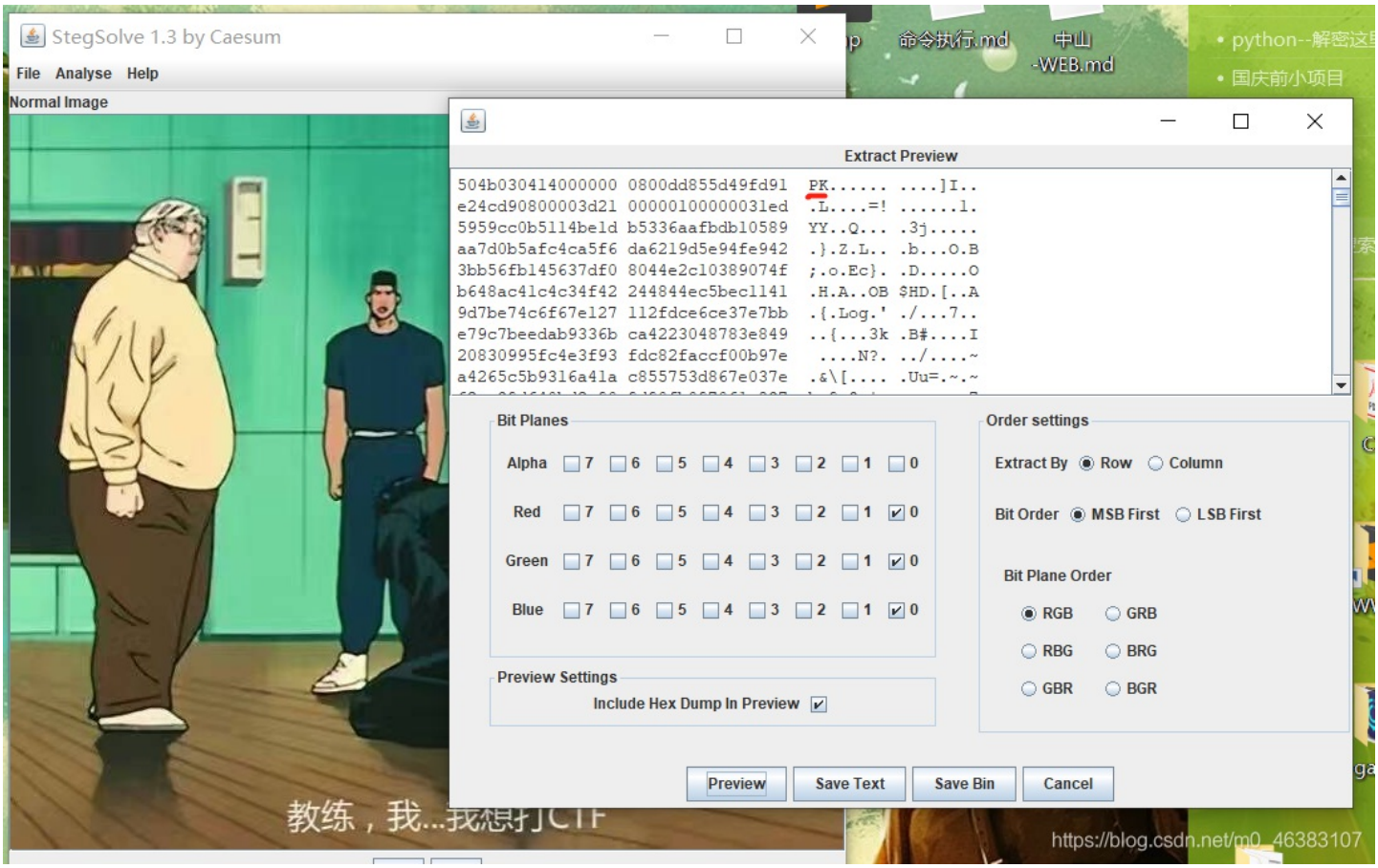
看第一个的追踪流直接出flag



FLAG

下载后是这个图片

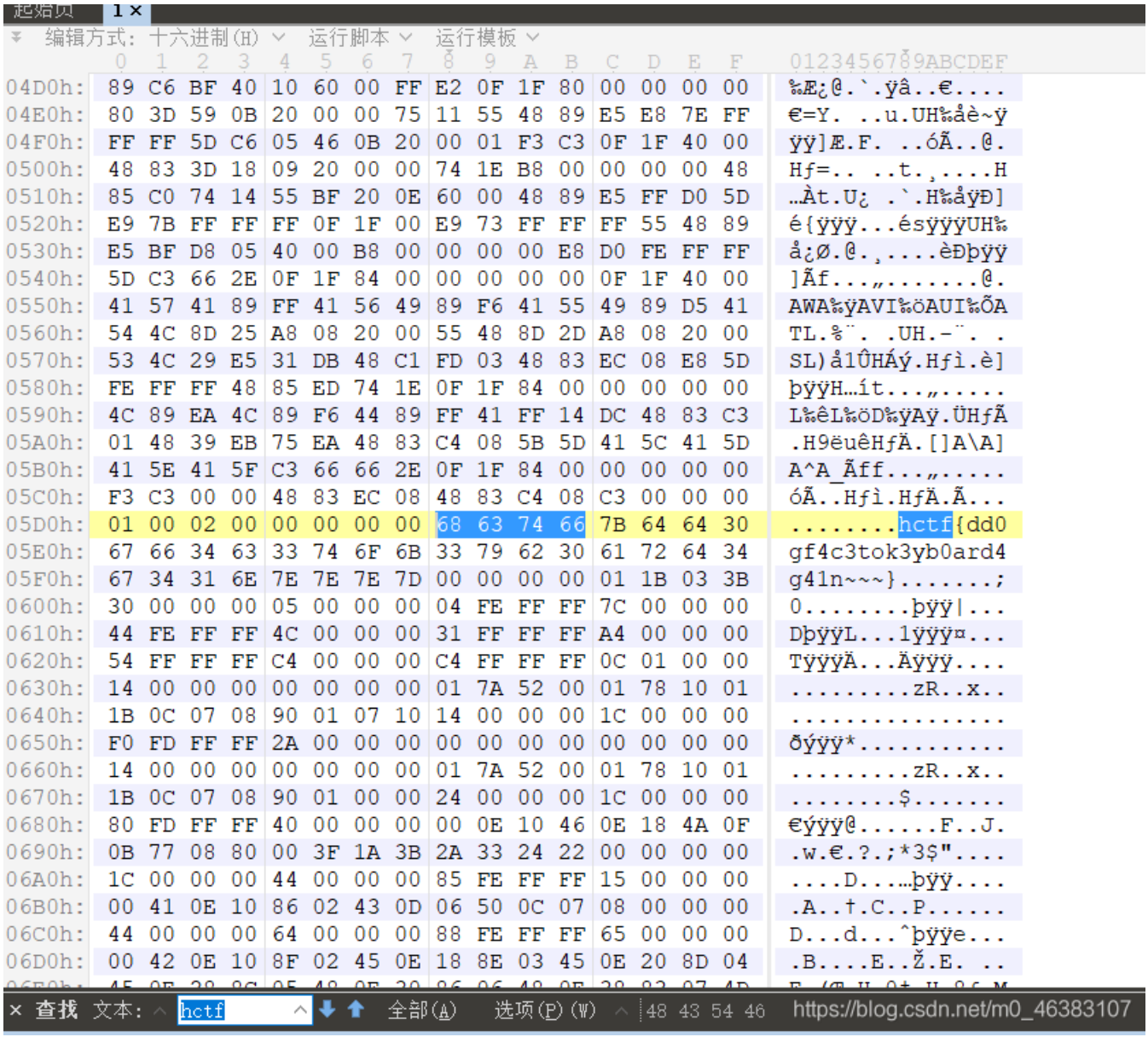

教练，我...我想打CTF
https://blog.csdn.net/m0_46383107



看到pk 用zip去解压

解压后丢进010editor

题目说的是hctf 所以去找hctf



另外一个世界

下载后是一张图片

丢进010里面 看到后面有101010这些二进制很可疑

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
2540h: 5A 34 F2 39 EE 47 0C 6F D0 7E DB 0E 4A B6 AE CD  Z4ò9îG.oÐ~Û.J¶®Í
2550h: 53 80 95 00 42 F2 9F 0E CA DC 7A 0F DB 6A 5E 27  S€•.BòŸ.ÊÜz.Ûj^'
2560h: 36 BE CF 50 FE 1C 2B 83 DF 97 75 77 04 FF 00 EA  6¾ÏPþ.+ƒß—uw.ÿ.ê
2570h: 55 DC 3E 2A AD 87 0F 0F 95 53 E4 91 26 97 D1 C2  UÜ>*-‡..•Sä'&—ÑÂ
2580h: FF 00 E4 4E D6 52 8B AA DA BB 3D 6F AB F3 94 2C  ÿ.äNÖR‹ªÚ»=o«ó",
2590h: 47 BA 84 3F F0 FB B6 14 B5 1F BF AC A1 46 48 E8  G°„?ðû¶.µ.¿¬¡FHè
25A0h: D5 F4 AF A0 13 F9 7B FE 55 81 C3 C3 E5 41 CD B3  Õô¯ .ù{þU.ÃÃåAÍ³
25B0h: 2A 47 12 4F A1 0D AA 84 80 36 BD 8F 02 AE A2 F3  *G.O¡.ª„€6½..®¢ó
25C0h: 20 77 76 54 87 D0 B6 D7 2A 52 95 B6 AC D2 09 C4   wvT‡Ð¶×*R•¶¬Ò.Ä
25D0h: A0 96 D7 99 1F DA BB 49 E3 E3 F3 AC 2F D5 57 71  –×™.Ú»Iãã ó¬/ÕWq
25E0h: F9 D3 7C B3 40 71 4F D1 C6 5D F4 2D B5 D4 94 A1  ùÓ|³@qOÑÆ]ô-µÔ"¡
25F0h: BD AF 64 80 91 21 3D 1A B3 3C 3C 2B A1 6E 1E EE  ½¯d€'!=.³<<+¡n.î
2600h: 5C EE AE EE 33 B2 AE AE 9B B9 79 0E B8 E1 71 A0  \î®î3²®®›¹y.¸áq
2610h: 40 21 46 78 F7 D5 A0 FE F0 79 E7 51 35 FB F5 7F  @!Fx÷Õ þðyçQ5ûõ.
2620h: 48 F8 0A 59 E4 94 BB 1A 29 30 31 31 30 31 30 31  Hø.Yä"».)0110101
2630h: 31 30 31 31 30 31 31 31 31 30 31 31 30 30 31 30  1011011110110010
2640h: 31 30 31 31 30 31 30 31 31 30 31 31 30 31 30 31  1011010110110101
2650h: 30 30 30 31 31 30 30 31 31 30 31 31 31 30 30 31  0001100110111001
2660h: 31 2E 00 00 00                                   1....
```

https://blog.csdn.net/m0_46383107

去这个网站解密http://ctf.ssleye.com/jinzhi.html

ASCII与2进制、10进制和16进制之间相互转；2进制、8进制、10进制、16进制及任意进制相互转换

ASCII ⇌ 进制　进制转换（常用）　进制转换（任意）

文本　koekj3s

清 空

二进制　01101011 01101111 01100101 01101011 01101010 00110011 01110011

https://blog.csdn.net/m0_46383107

得到的结果加上flag{koekj3s}

假如给我三天光明

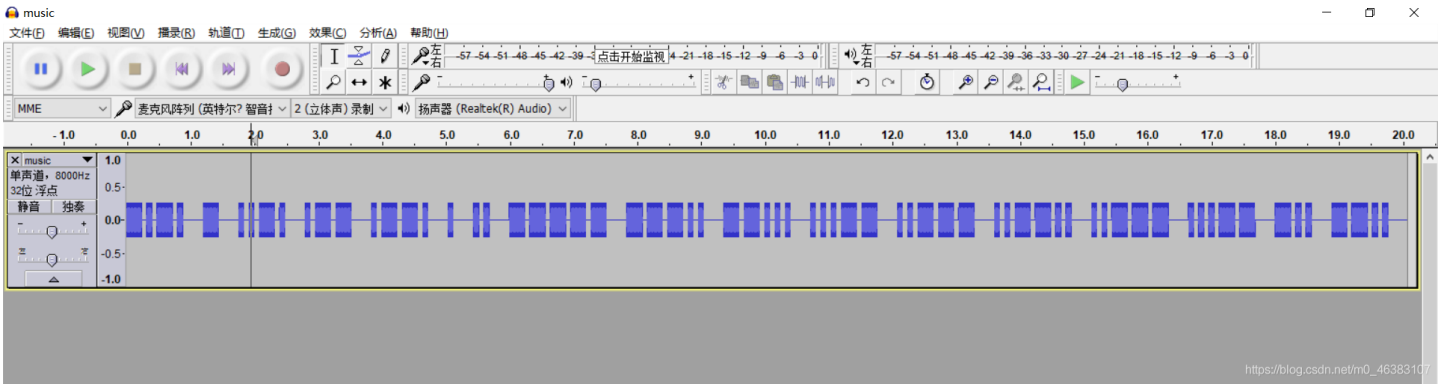
有两个东西 zip是加密文件， 应该是要用jpg去找到密码

在图片下面有黑点 （盲文）

对比解密后是kmdonowg

里面是音频

用Audacity打开



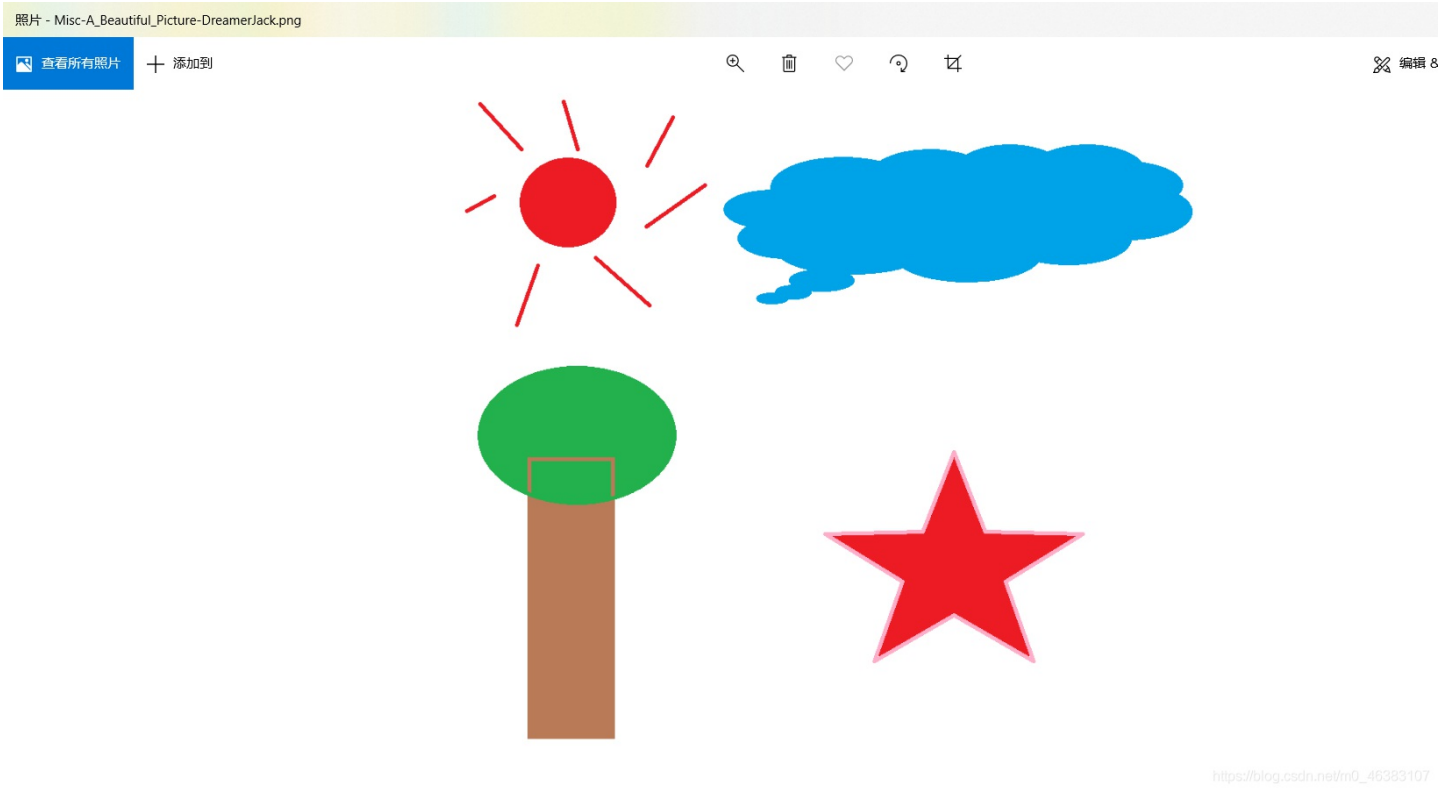
看出来是摩斯密码

-.-. - …-. .-- .–. . … ----- —… …-- …— …–… …— …-- -… --…

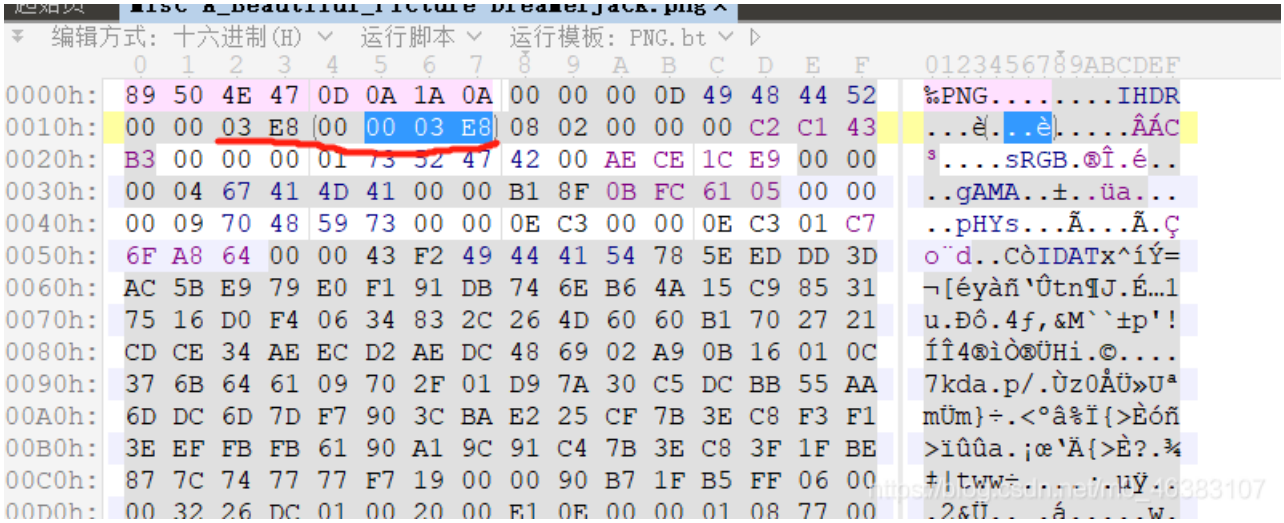
去解密得到的可能是大写字母 最后要改一下

flag{wpei08732?23dz}

A_Beautiful_Picture

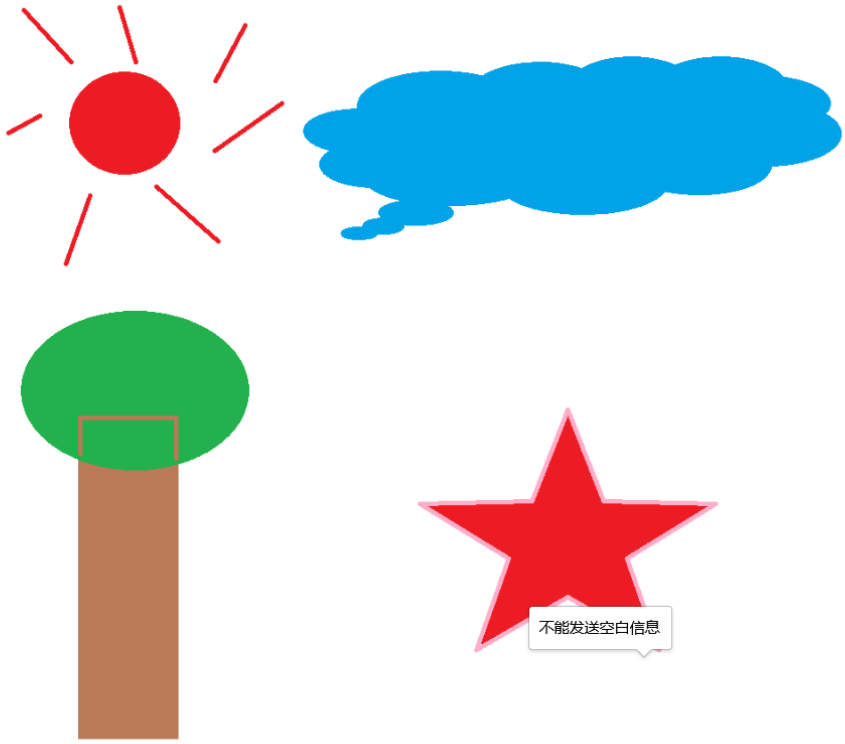


看上去没什么东西，可能长度有点问题，尝试去修改一下，改成长宽一样就出来falg



tiful_Picture-DreamerJack.png

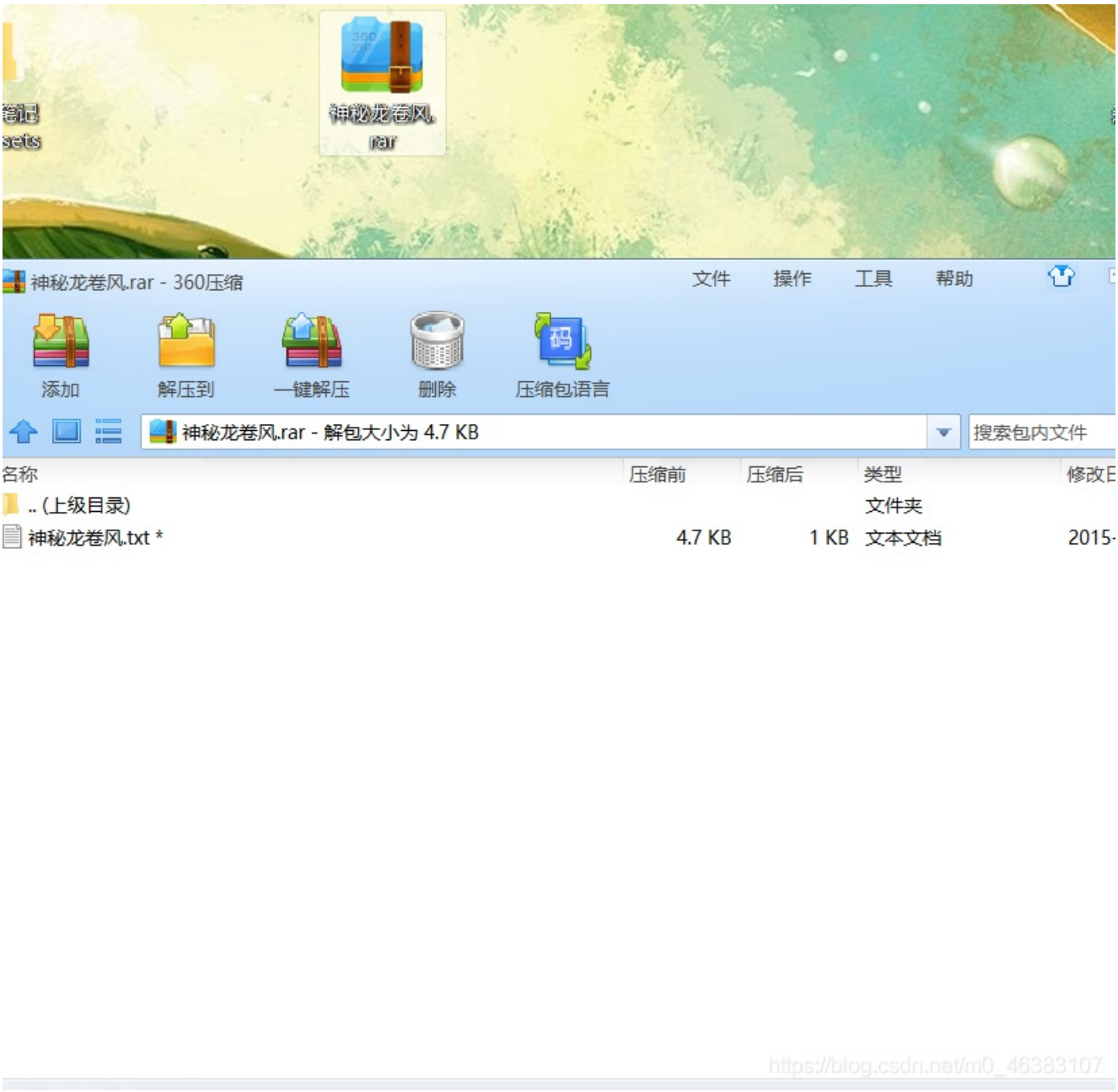
添加到



BJD{PnG_He1ghT_1s_WR0ng}

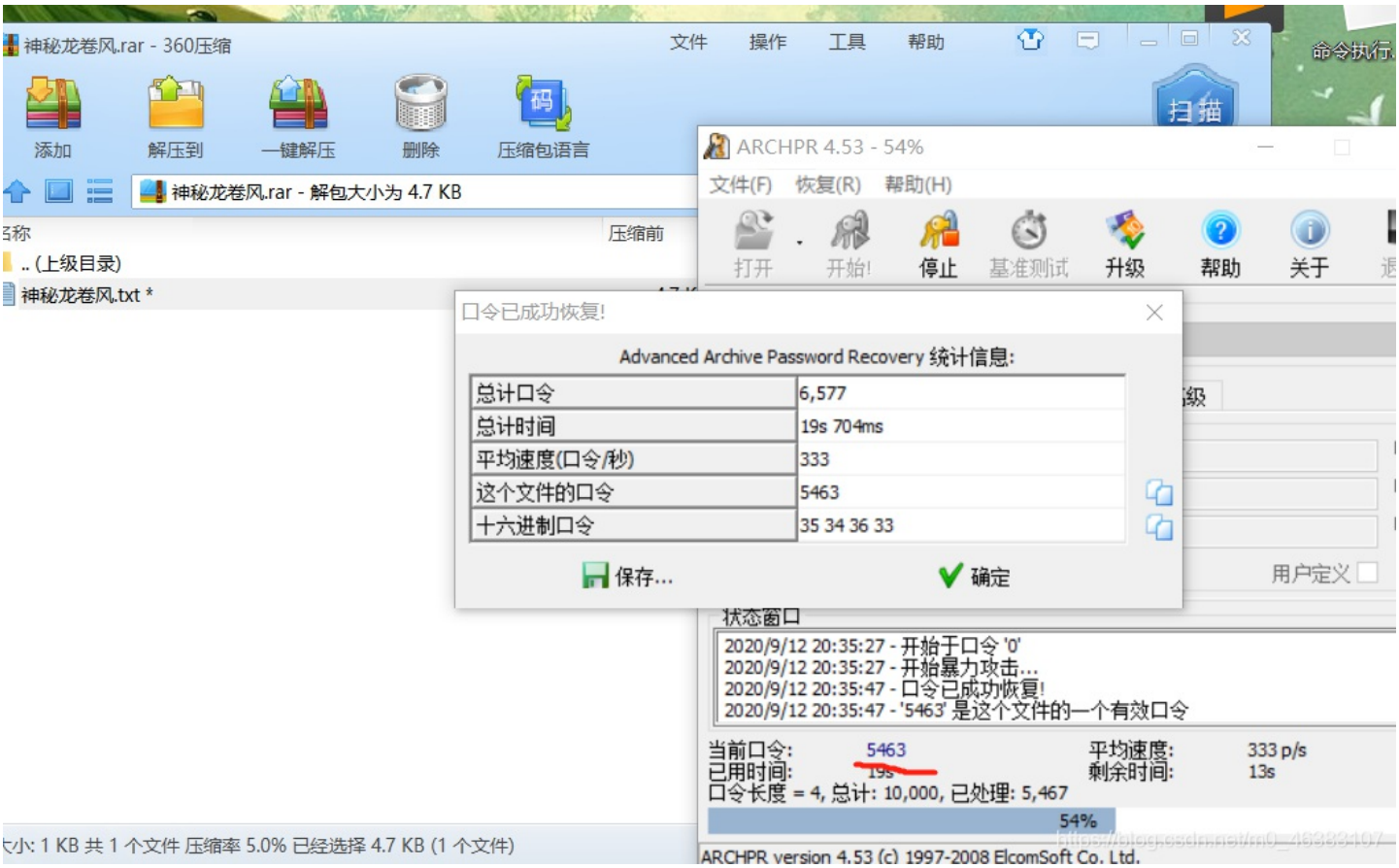
https://blog.csdn.net/m0_46383107

神秘龙卷风

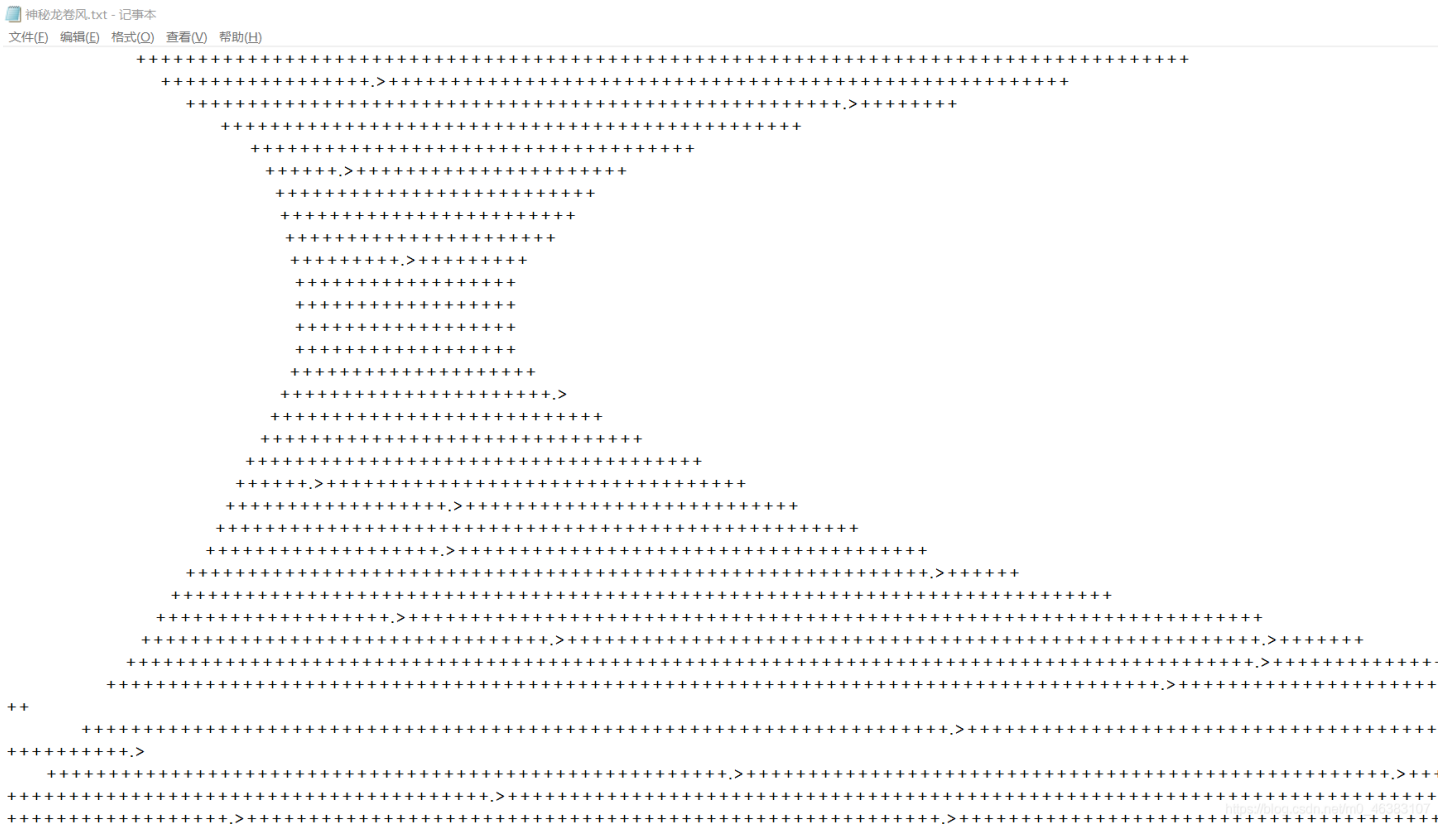


https://blog.csdn.net/m0_46383107

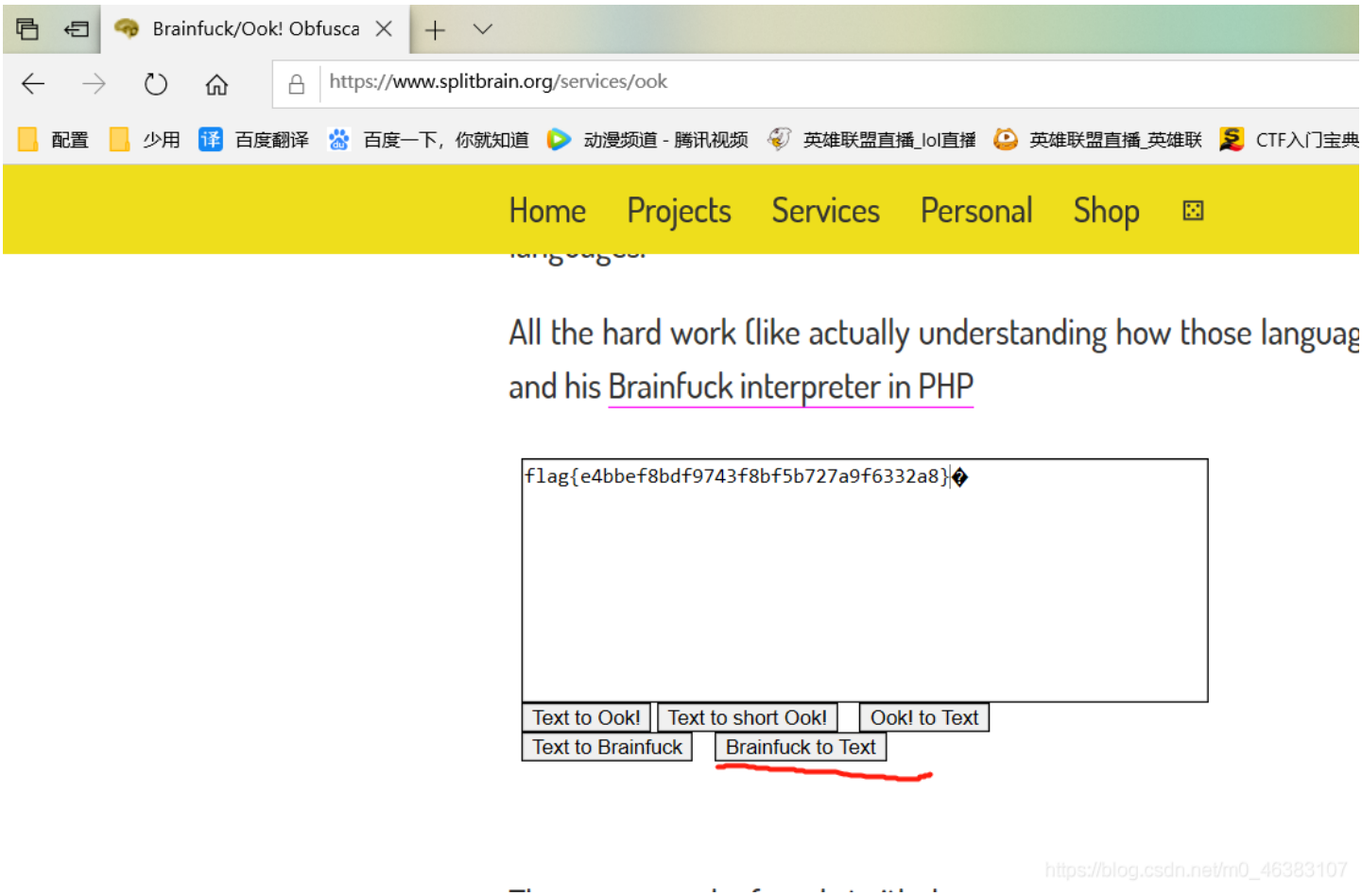
破解rar 因为是4为纯数字 直接暴力破解



打开文件，看到这个奇奇怪怪的东西，想去破解他



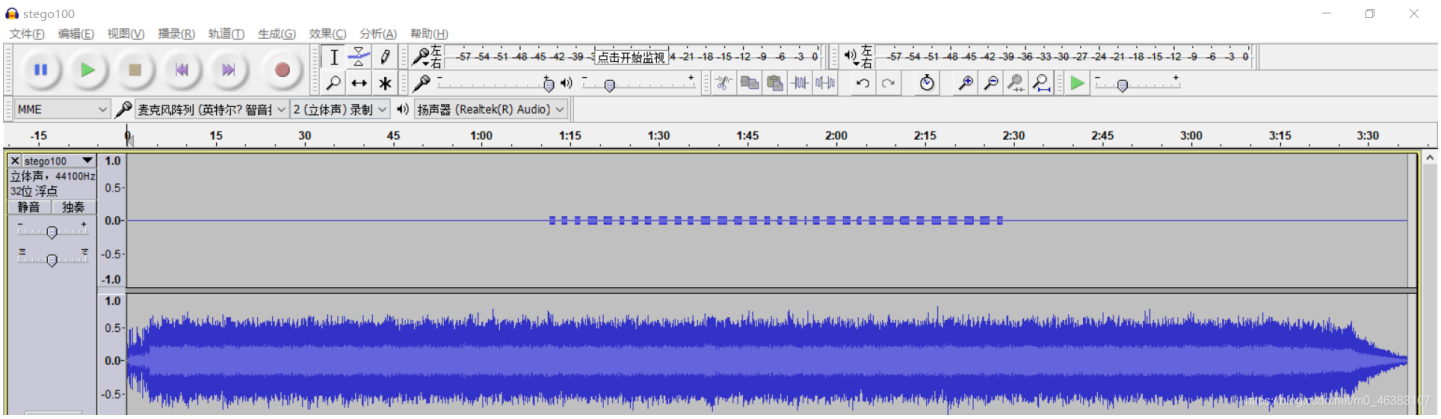
https://www.splitbrain.org/services/ook去这个网站就可以解密

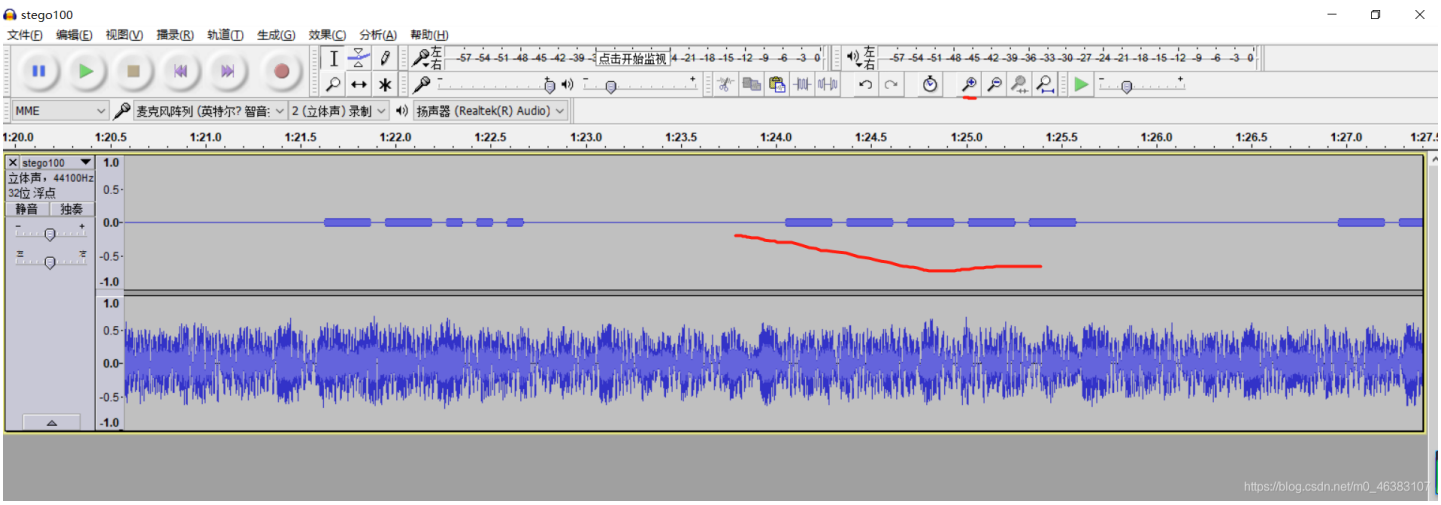


https://blog.csdn.net/m0_46383107

来首歌吧

打开是一个音频





… -… -.- ----. …— … -… …- ----. -.-. -… ----- .---- —… —… …-. … …— . -… .---- --… -… --… ----- ----. …— ----. .---- ----. .---- -.-.

弄出了摩斯密码去解密，得到下面的结果加个falg{}就可以