第二届“金盾信安杯”网络安全大赛misc部分wp

原创

没用的阿吉1 于 2021-02-06 12:54:53 发布 346 收藏 2

分类专栏： ctf

本文链接：https://blog.csdn.net/qq_48621670/article/details/113716361

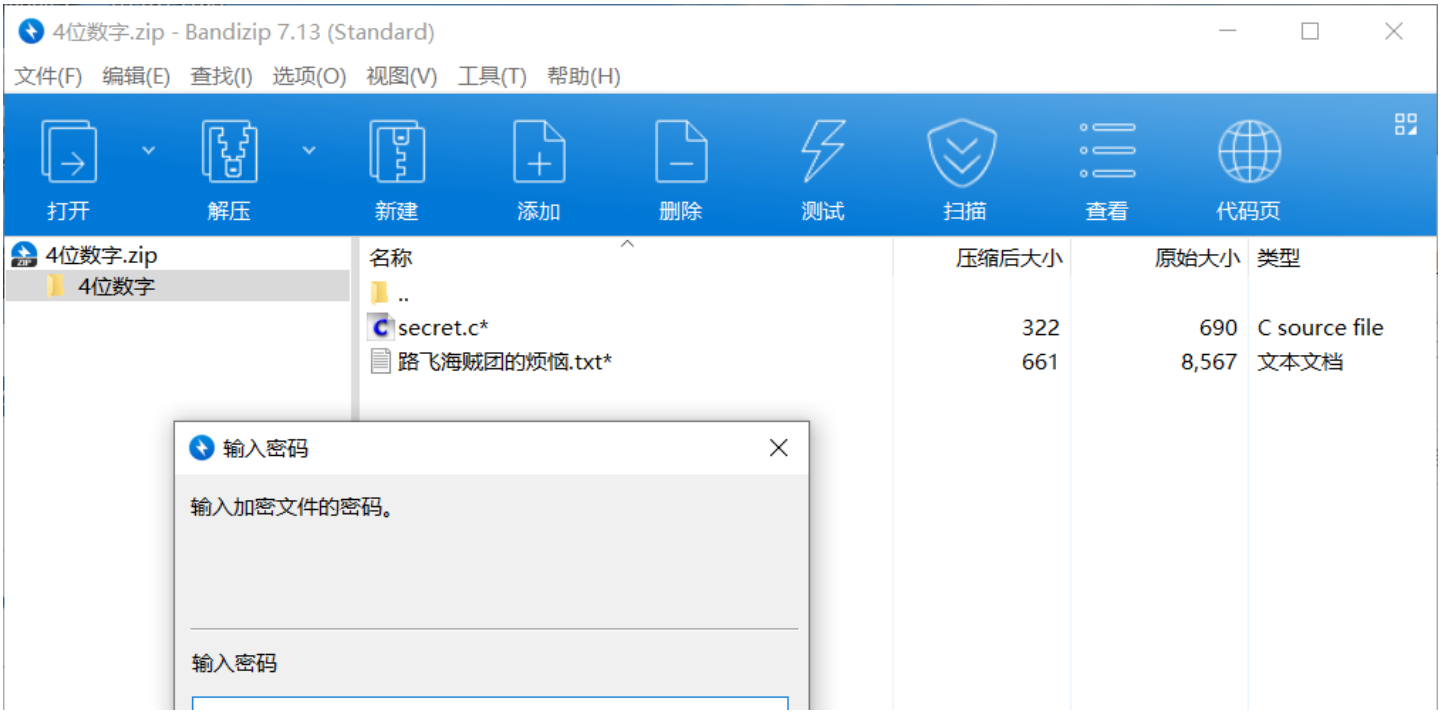
文章目录

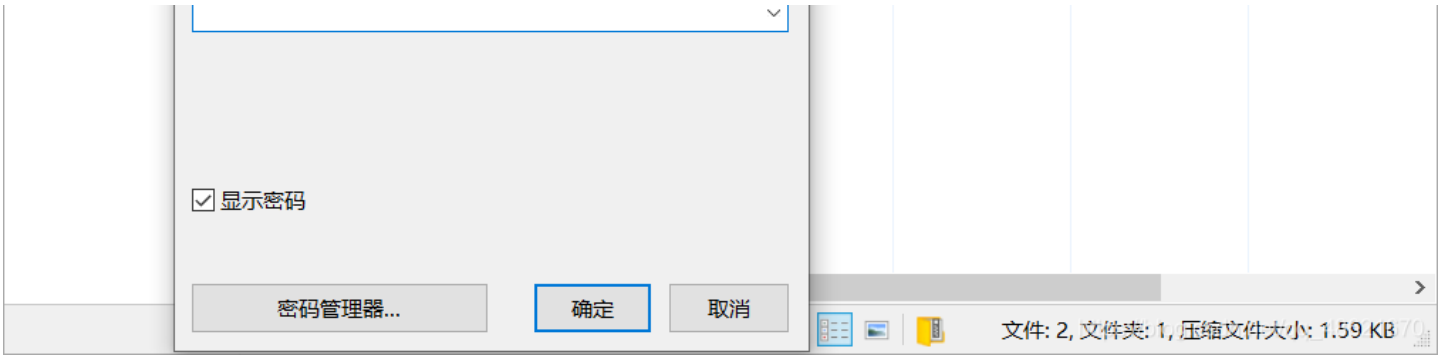
前言

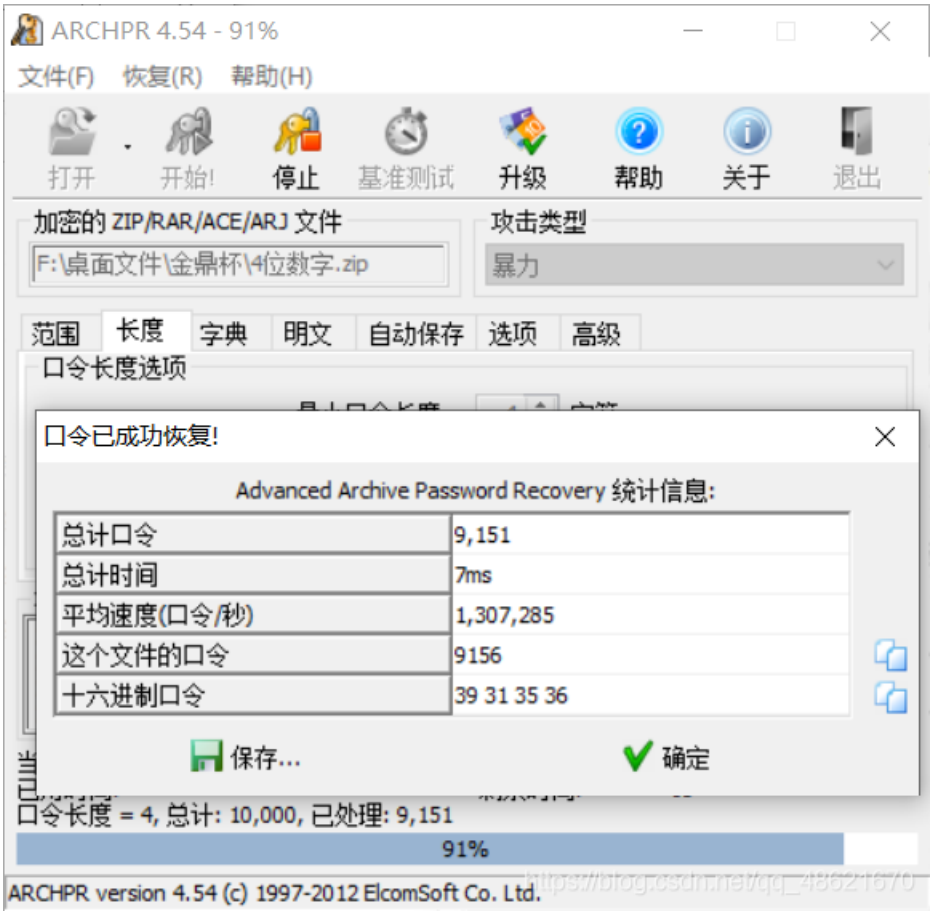
全为miscwp

一、4位数字

下载后得到一个压缩包，打开需要密码，文件名已经提示为四位数字，所以直接上ARCHPR进行爆破

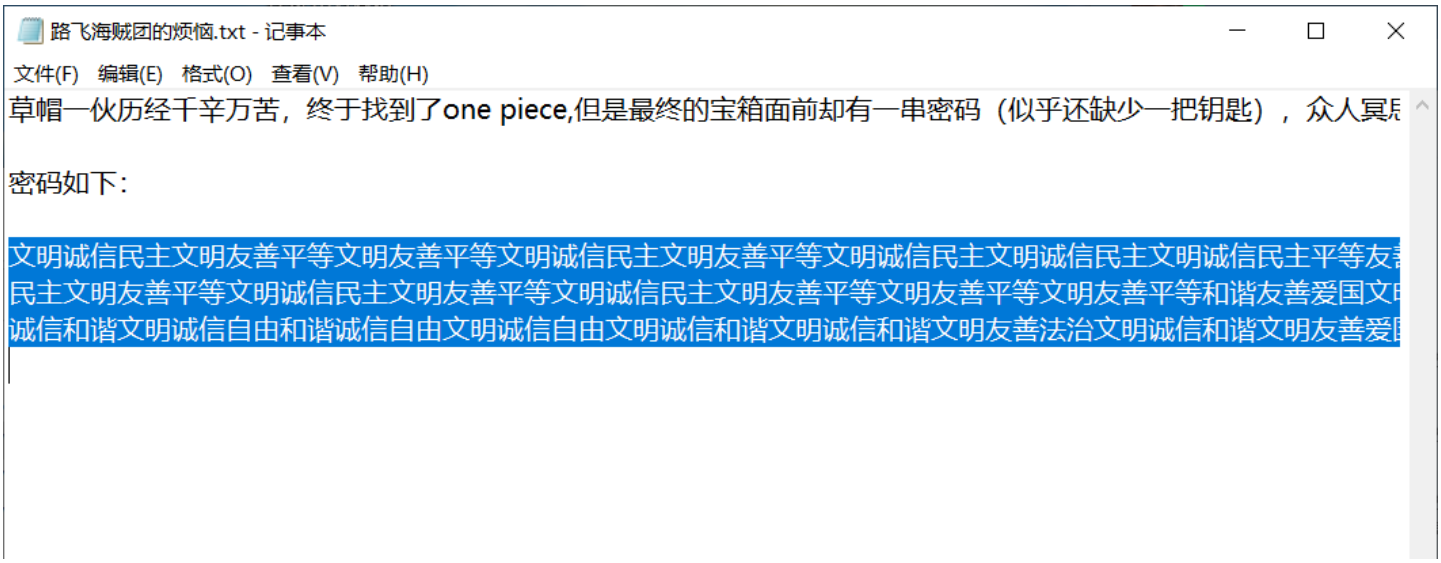


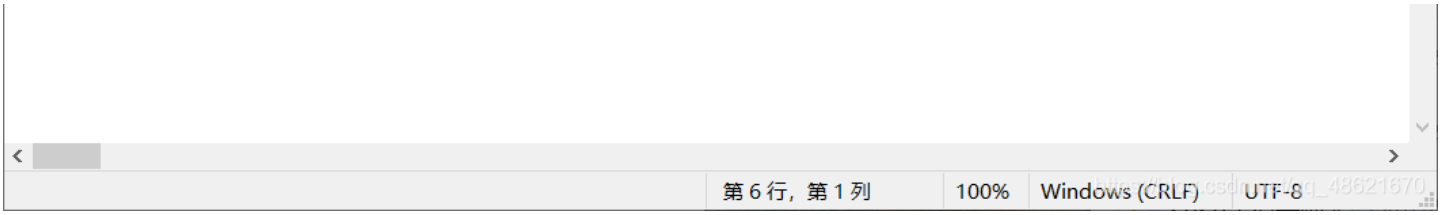




爆破拿到密码**9156**

打开后是两个文件





here | secret.c

```c
#include <stdio.h>

int main()
{
    unsigned int first, second, thirdly, fourthly;

    if (first + 2 != 100)
    {
        printf("wrong!\n");
    }

    if (second * second != 9409)
    {
        printf("Made a mistake!\n");
    }

    if (thirdly / 7 == 14 && thirdly < 100)
    {
        printf("yes! You got it\n");
    }

    if (fourthly != 121)
    {
        printf("not this!\n");
    }

    int p[4] = {first,second,thirdly,fourthly};
    int i;

    printf("key:");
    for ( i = 0; i < 4; i++)
    {
        printf("%c", p[i]);
    }

    printf("\n");
    return 0;
}
```


在路飞的烦恼中直接看到社会主义核心价值观直接解密，贴上解密网址https://ctf.bugku.com/tool/cvecode解密后得到

++++++++

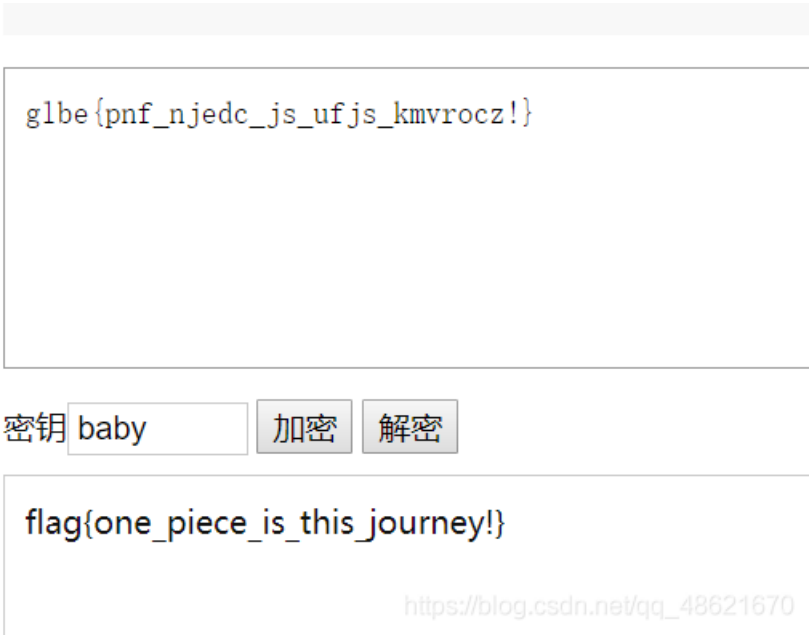
[>>++>++++>++++++>++++++++>++++++++++>++++++++++++>++++++++++++++>++++++++++++++++>++++++++++++++++++>++++++++++++++++++++>++++++++++++++++++++++>++++++++++++++++++++++++>++++++++++++++++++++++++++>++++++++++++++++++++++++++++>++++++++++++++++++++++++++++++>++++++++++++++++++++++++++++++++<<<<<<<<<<<<<<<<-]>>>>>>>++++++++.>----.<-----.+++.>>-----.<++++.-.<+.-------.>.----.-----.-.-.<.>+++++++.>--------.<<.>>++.<----.++++.>-.<<.>+.++.>+++.----.<++.<++++.>>++++++++.<<<<<<+.>>>>>>+++.

看编码形式为brainfuck编码，直接解码，再次贴上网址https://www.tutorialspoint.com/execute_brainfk_online.php，解码后得到glbe{pnf_njedc_js_ufjs_kmvrocz!}尝试提交但是错误，八嘎！flag在哪

让我们再来分析c语言源码，一通瞎鸡儿分析后，猜测让不等变成等于符合条件的ascll一下就出来了密码是baby

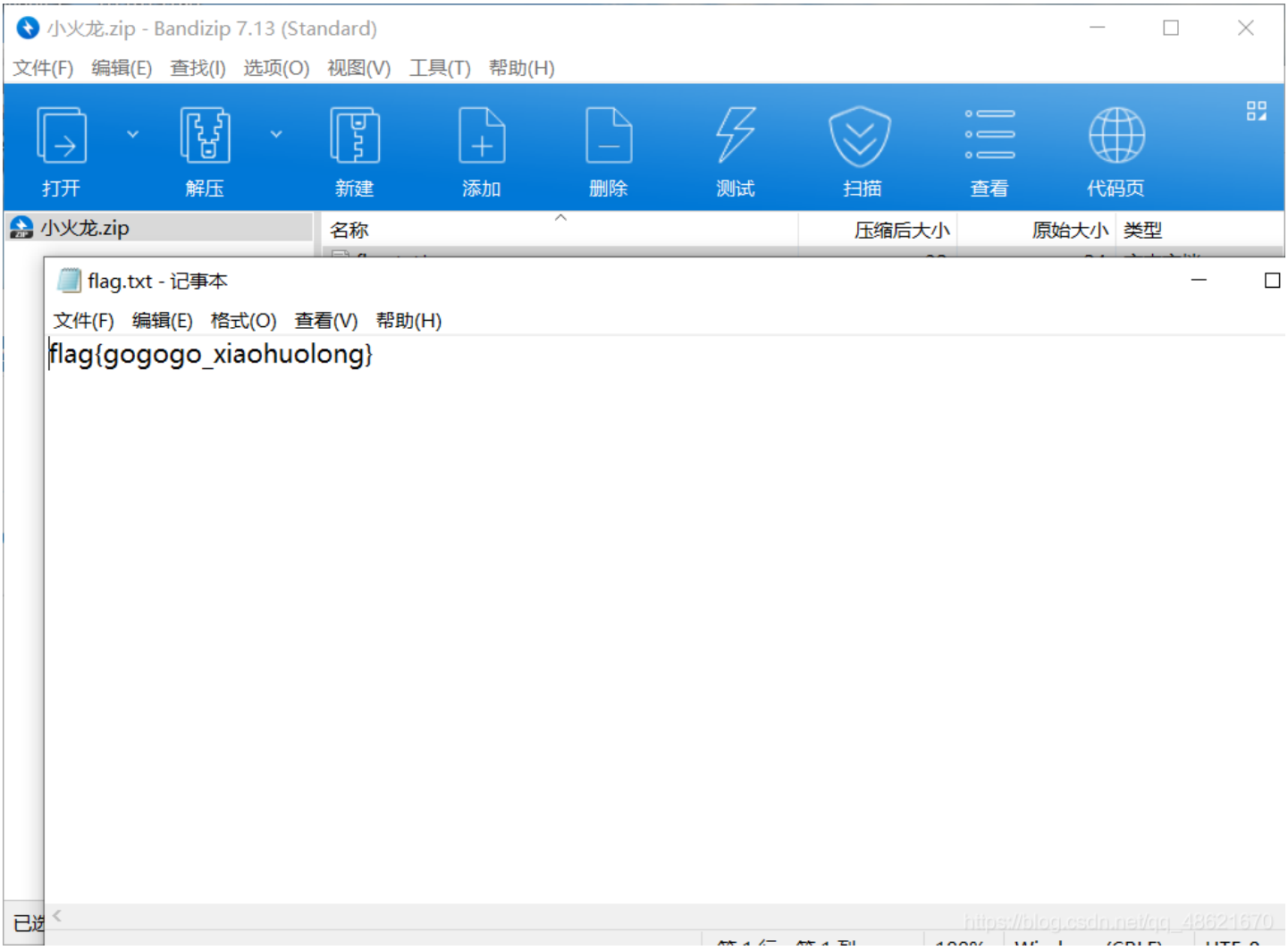
看来解密需要用到这个密码一通乱试之后，发现维吉尼亚密码出现了正确flag呦西！！！

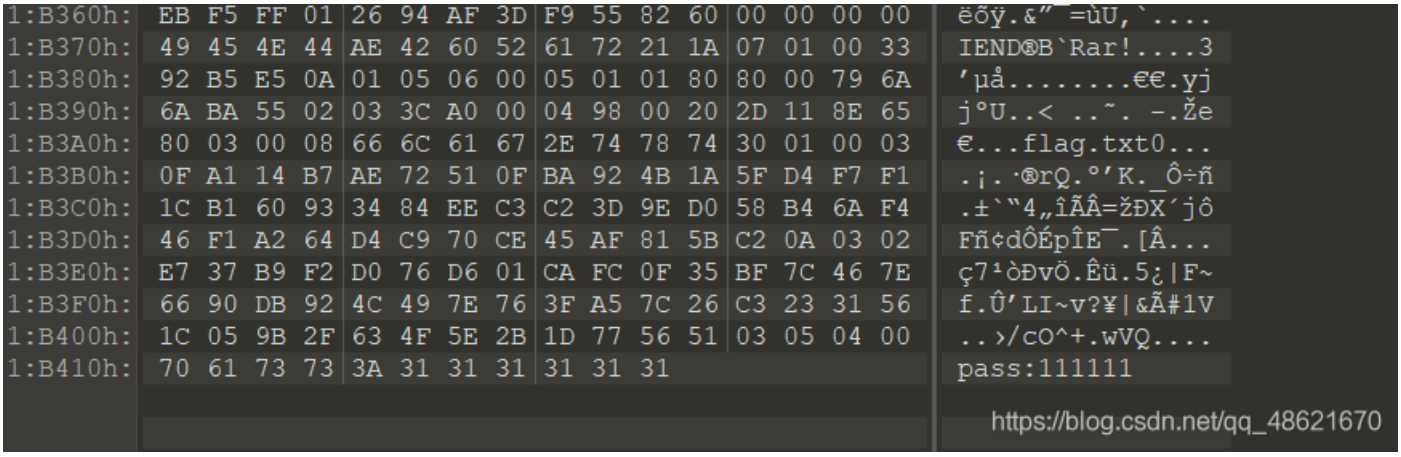
flag{one_piece_is_this_journey!}



二、小火龙

下载后得到一张图片放进010中看到尾部有密码，里面可能隐藏压缩包，直接更改后缀，得到压缩包，拿密码打开压缩包





得到flag

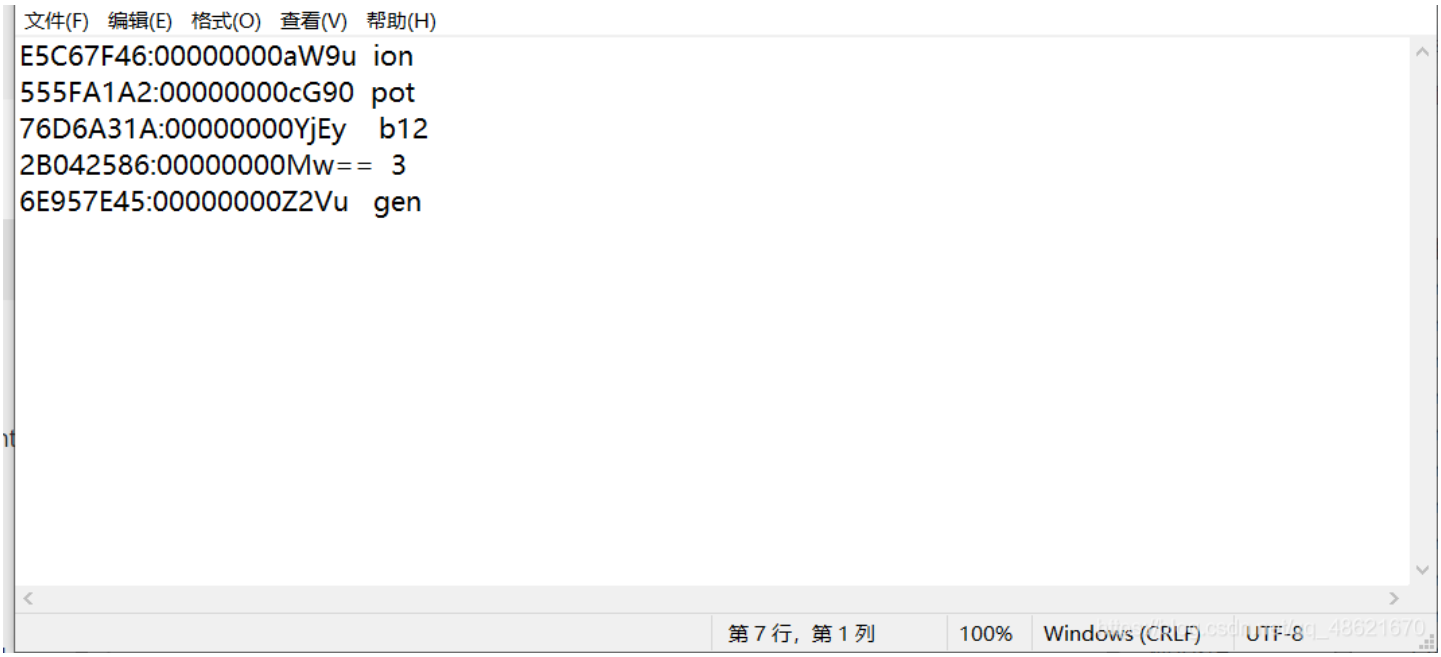
三、五瓶药水

下载后得到好多个压缩包观察文件大小可以猜测为crc碰撞

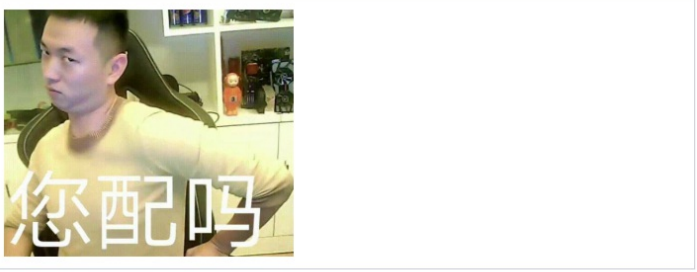
flag.zip	34 297	34 297	2020-09-0...	2020-09-0...	2020-09-0...	A	-	79CB3FAC	Store	NTFS : UTF8 FAT	10
橙色.zip	170	170	2020-09-0...	2020-09-0...	2020-09-0...	A	-	F5E05FAA	Store	NTFS : UTF8 FAT	10
红色.zip	170	170	2020-09-0...	2020-09-0...	2020-09-0...	A	-	DBF3D027	Store	NTFS : UTF8 FAT	10
绿色.zip	170	170	2020-09-0...	2020-09-0...	2020-09-0...	A	-	B6E8CBB1	Store	NTFS : UTF8 FAT	10
青色.zip	170	170	2020-09-0...	2020-09-0...	2020-09-0...	A	-	769FF178	Store	NTFS : UTF8 FAT	10
黄色.zip	170	170	2020-09-0...	2020-09-0...	2020-09-0...	A	-	C604135B	Store	NTFS : UTF8 FAT	10

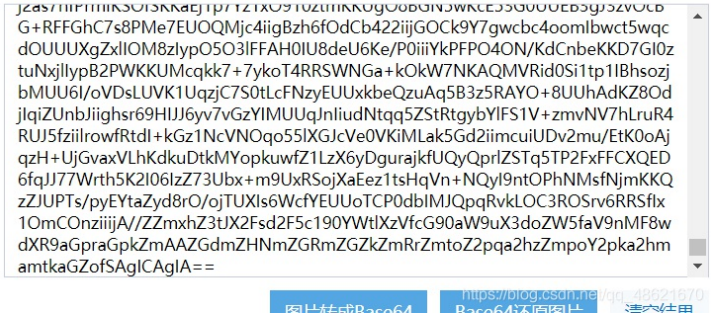
打开压缩包记住crc值记住填入到填入hashcat中crc.txt中，打开cmd命令运行hashcat.exe -m 11500 -a 3 crc.txt ?a?a?a?a?a?a -i --increment-min 4 --increment-max 5 --outfile-autohex-disable -o pa.txt --force --keep-guessing

最后得到用红橙黄绿青蓝紫排一下顺序得到**potiongenb123**用密码打开压缩包

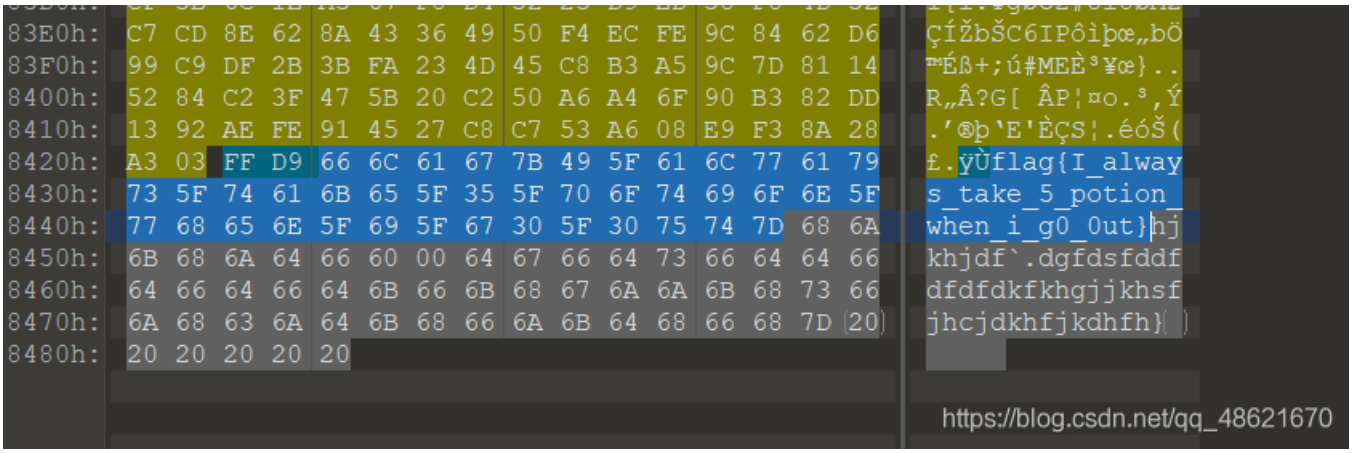


用base转图片得到





把图片保存下来在010中打开得到



flag{I_always_take_5_potion_when_i_g0_0ut}