# buu 7.15

原创

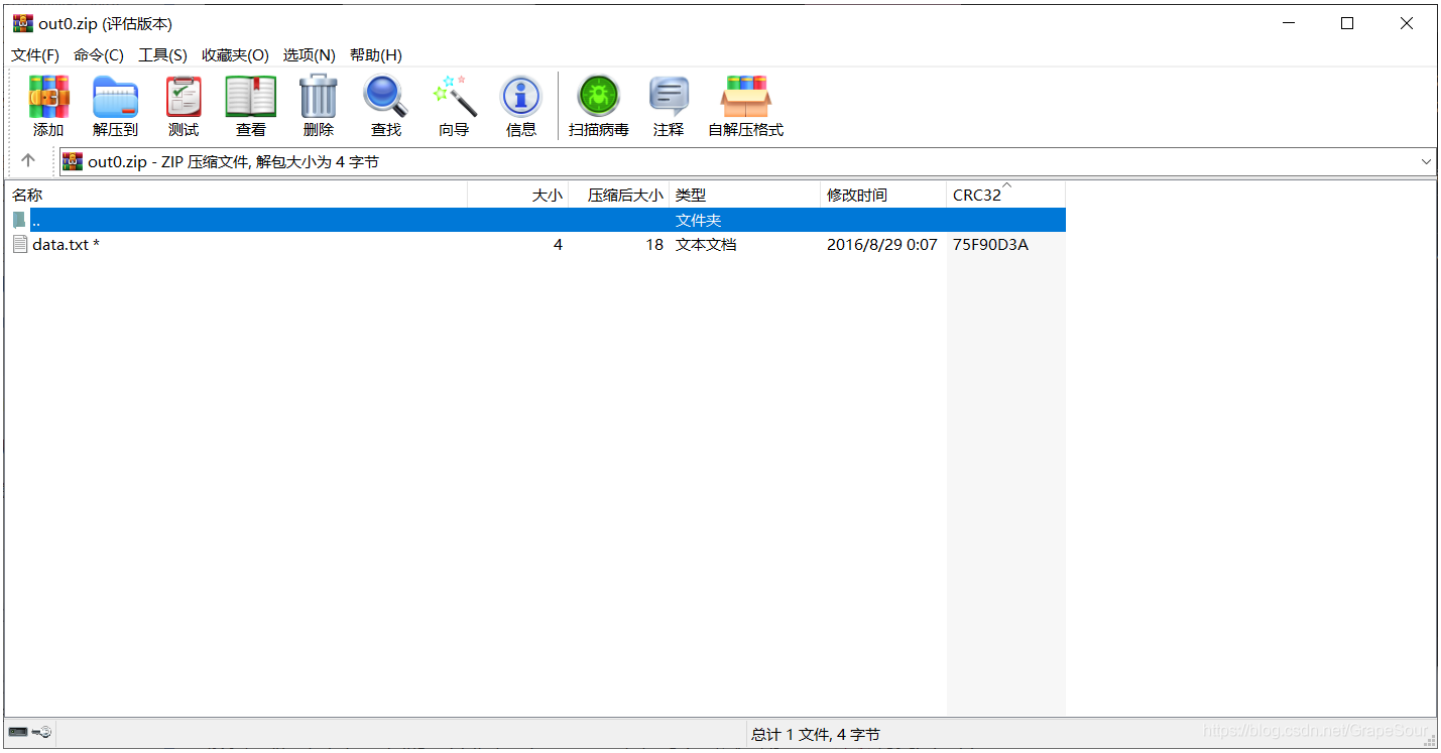
GrapeSour 于 2021-07-15 19:58:01 发布 76 收藏 1


## buu刷题



## zip

打恺压缩包，发现里面有很多加密压缩包，但是里面的内容非常小，小于5字节，可以尝试使用CRC32爆破得到其内容



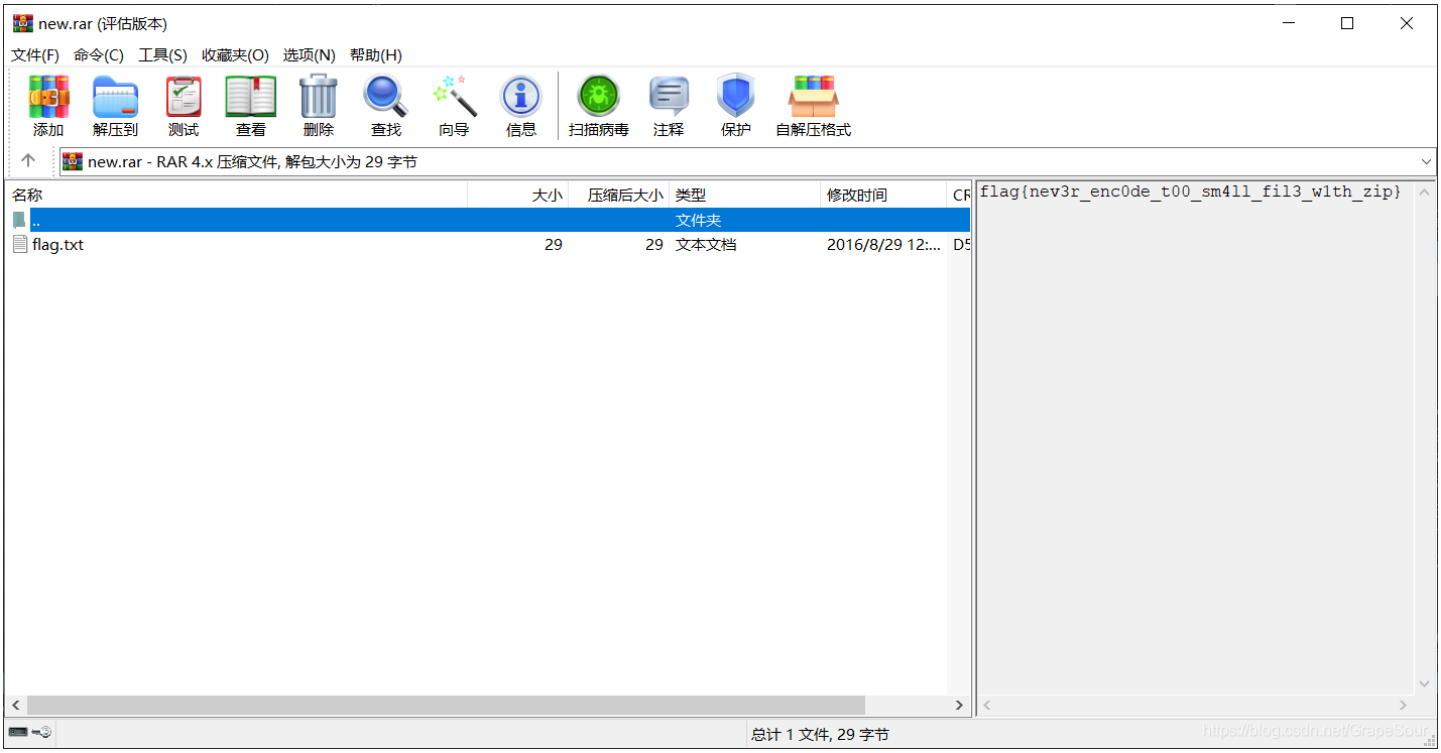

发现是base64编码，解码得到


是rar文件

010打开，添加rar文件头

```
52 61 72 21 1A 07 00
```

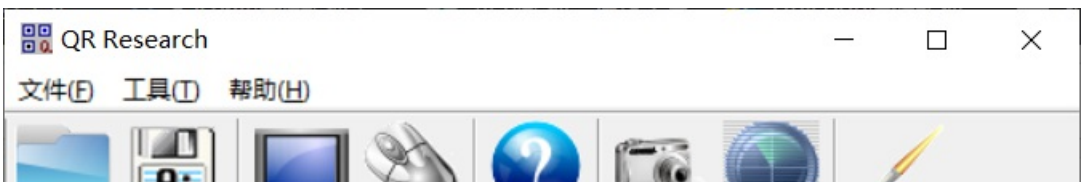
在注释中发现flag




## [RoarCTF2019]黄金6年

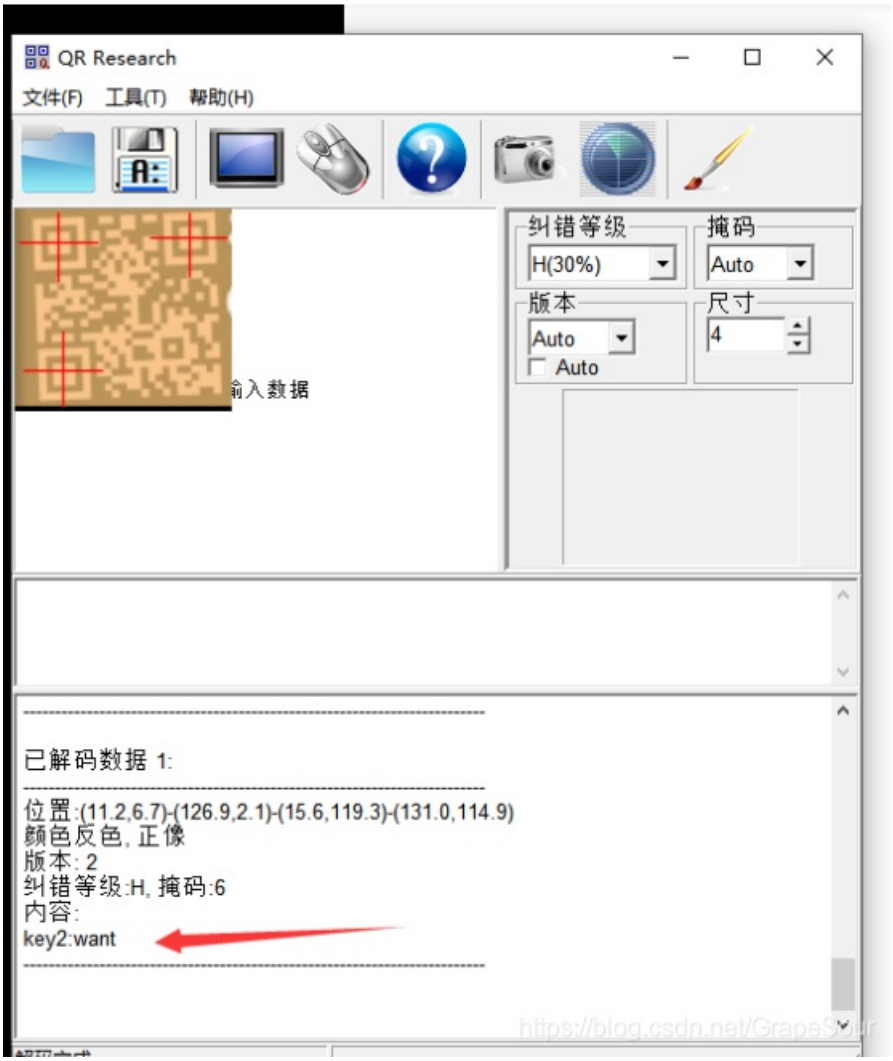
查看文件尾发现base64编码


存出来，发现需要密码，去视频里面慢慢找

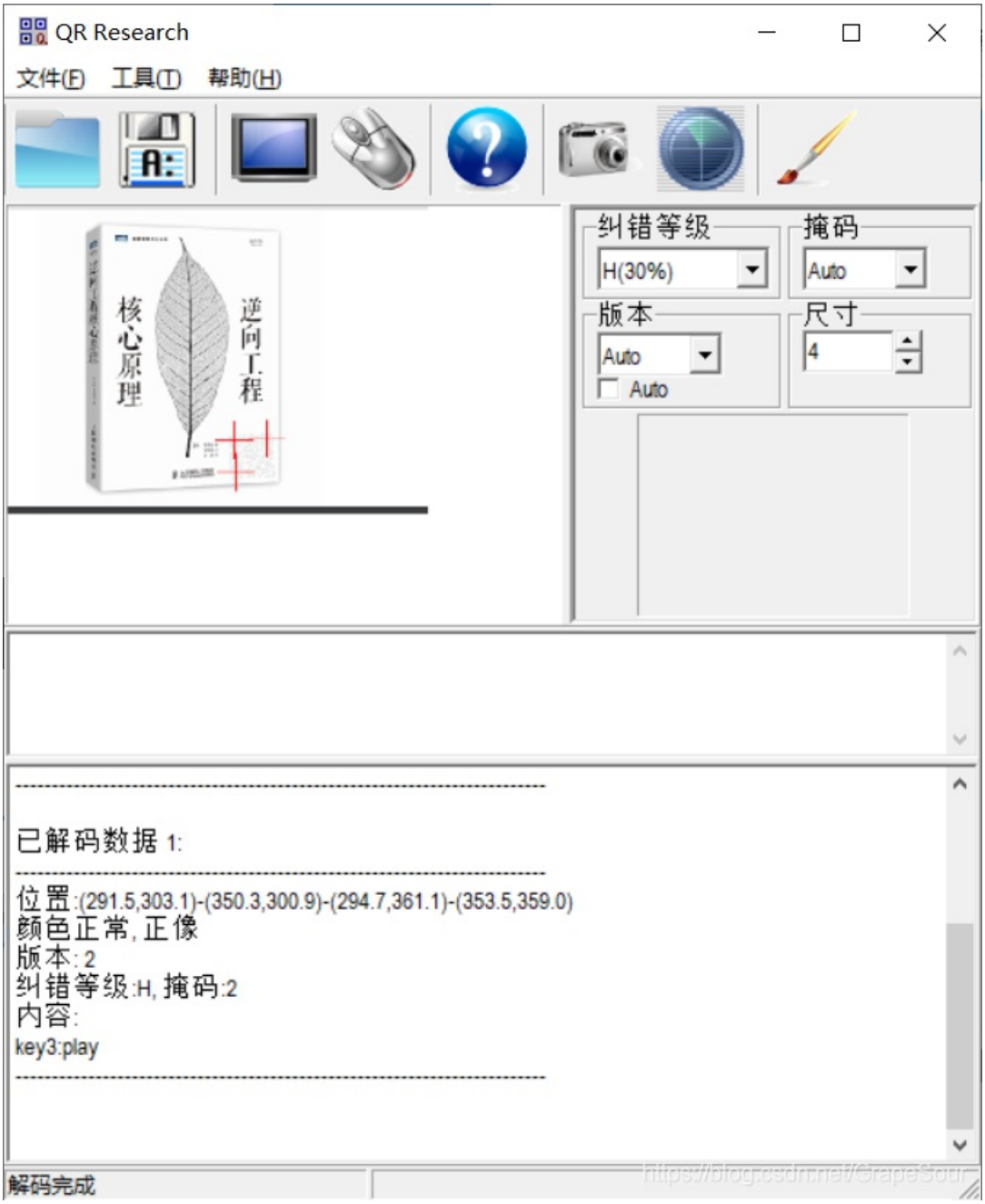



C++
Primer Plus
（第6版）中文版
请输入数据
纠错等级
H(30%)
掩码
Auto
版本
Auto
Auto
尺寸
4
已解码数据 1:
位置:(162.0,35.0)-(216.0,35.0)-(162.0,89.0)-(215.9,89.0)
颜色正常, 正像
版本: 1
纠错等级:H, 掩码:3
内容:
key1:i
解码完成

```
key1:i
```

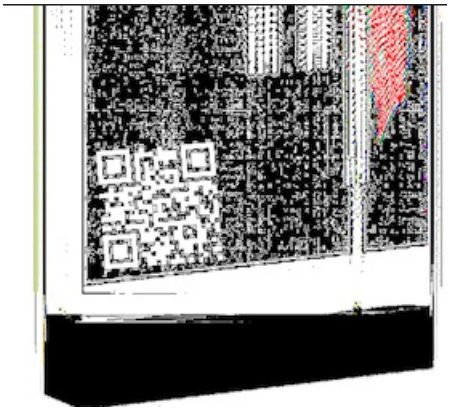

QR Research
文件(F) 工具(T) 帮助(H)
纠错等级
H(30%)
掩码
Auto
版本
Auto
Auto
尺寸
4
输入数据
已解码数据 1:
位置:(11.2,6.7)-(126.9,2.1)-(15.6,119.3)-(131.0,114.9)
颜色反色, 正像
版本: 2
纠错等级:H, 掩码:6
内容:
key2:want

```
key2:want
```




```
key3:play
```

中间有个坑。。。最后一张二维码背景是黑的根本找不到！！！（做题的时候根本没找到，还是根据黄金6年的梗猜出来的内容。。。后来看大神题解才知道在哪）



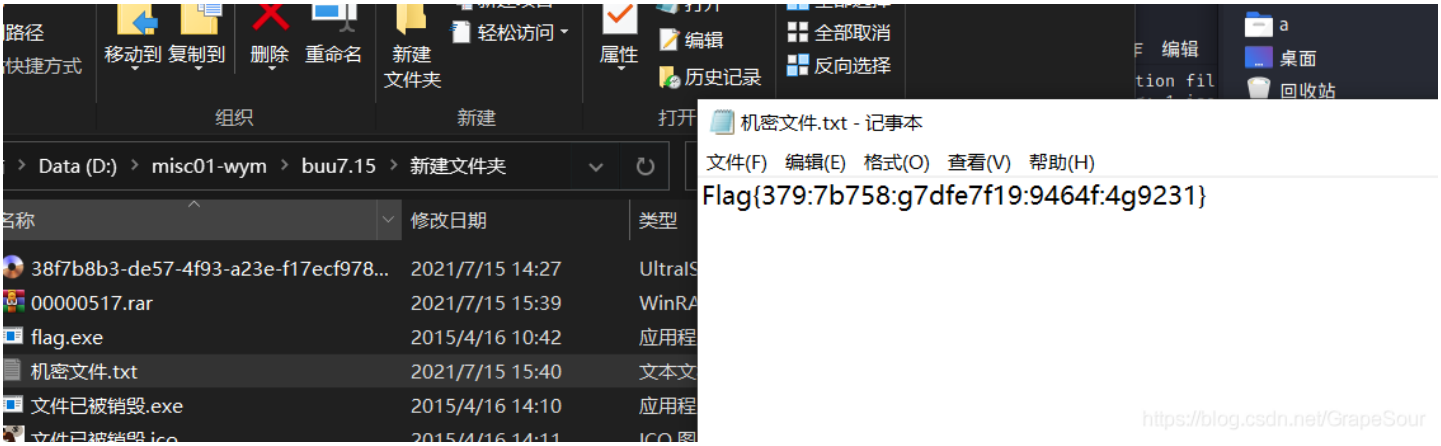
所以密码是

iwantplayctf

得到flag

## 间谍启示录

foremost分离得到一个rar文件
解压得到flag.exe
机密文件里就是flag




## [安洵杯 2019]吹着贝斯扫二维码

二维码拼图后得到密码
扫描得到

> BASE Family Bucket ???
> 85->64->85->13->16->32

查看压缩包发现注释

```
GNATOMJVIQZUKNJXGRCTGNRTGI3EMNZTGN
```

然后按照顺序来
是逆着的顺序

> base32->十六进制解码->ROT13->base85->base64->base85

```
GNATOMJVIQZUKNJXGRCTGNRTGI3EMNZTGNBTKRJWGI2UIMRRGNBDEQZWGI3DKMSFGNCDMRJTII3TMNBQGM4TERRTGEZTOMRXGQYDGOBWGI2DCNBY
```

编码 解码 清空

3A715D3E574E36326F733C5E625D213B2C62652E3D6E3B7640392F3137274038624148



> 在线工具 > 字符串和16进制互转工具

:q]>WN62os<^b]!;,be.=n;v@9/17'@8bAH

:q]>WN62os<^b]!;,be.=n;v@9/17'@8bAH

↓

ROT13

↓

:d]>JA62bf<^o]!;,or.=a;i@9/17'@8oNU



:d]>JA62bf<^o]!;,or.=a;i@9/17'@8oNU

PCtvdWU4VFJnQUByYy4mK1lraTA=



base16、base32、base64

PCtvdWU4VFJnQUByYy4mK1lraTA=

编码 base64 字符集 utf8(unicode

编

<+oue8TRgA@rc.&+Yki0



在线base65编码、在线base65解码、base65编码、base65解码

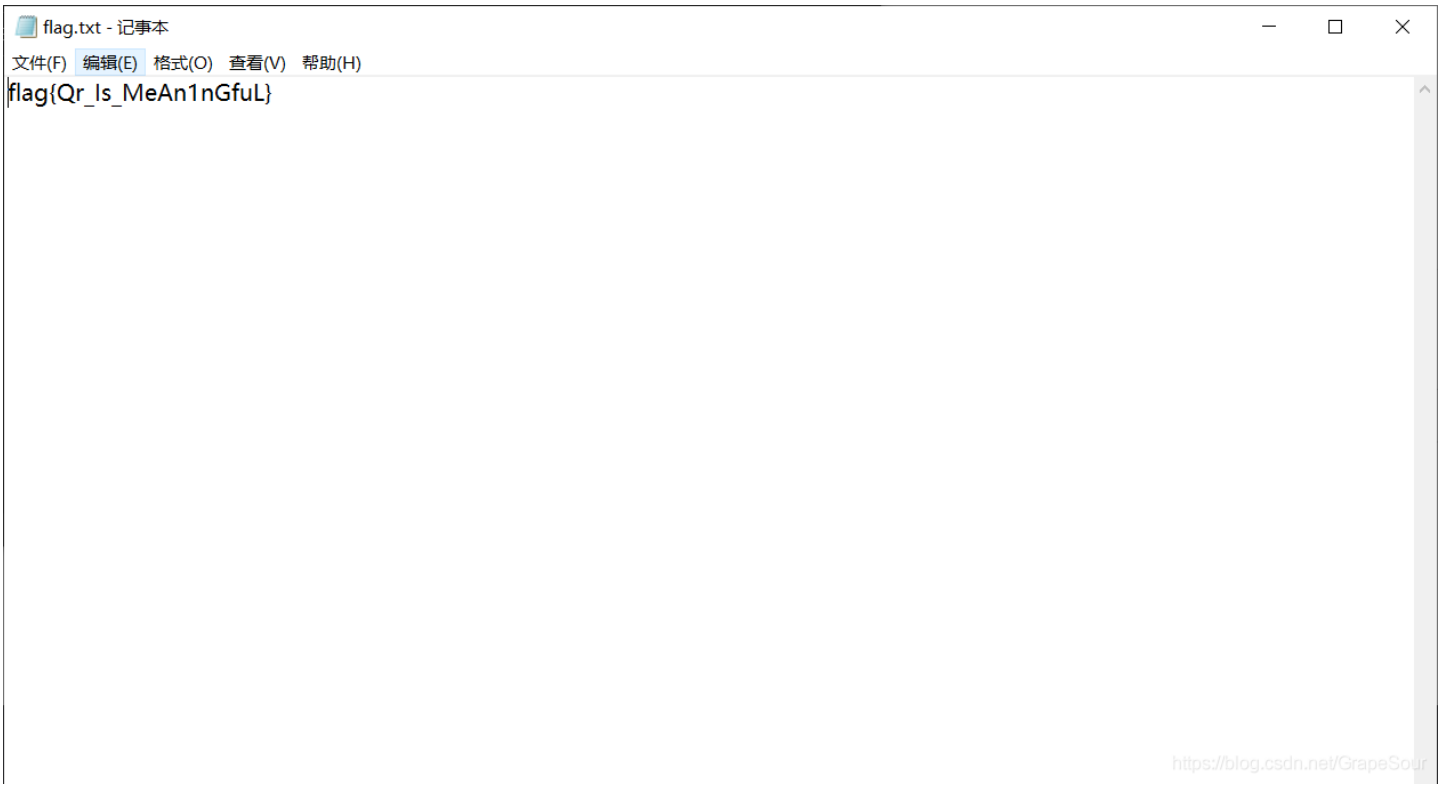
<+oue8TRgA@rc.&+Yki0

```
ThisIsSecret!233
```



得到压缩包密码

得到flag



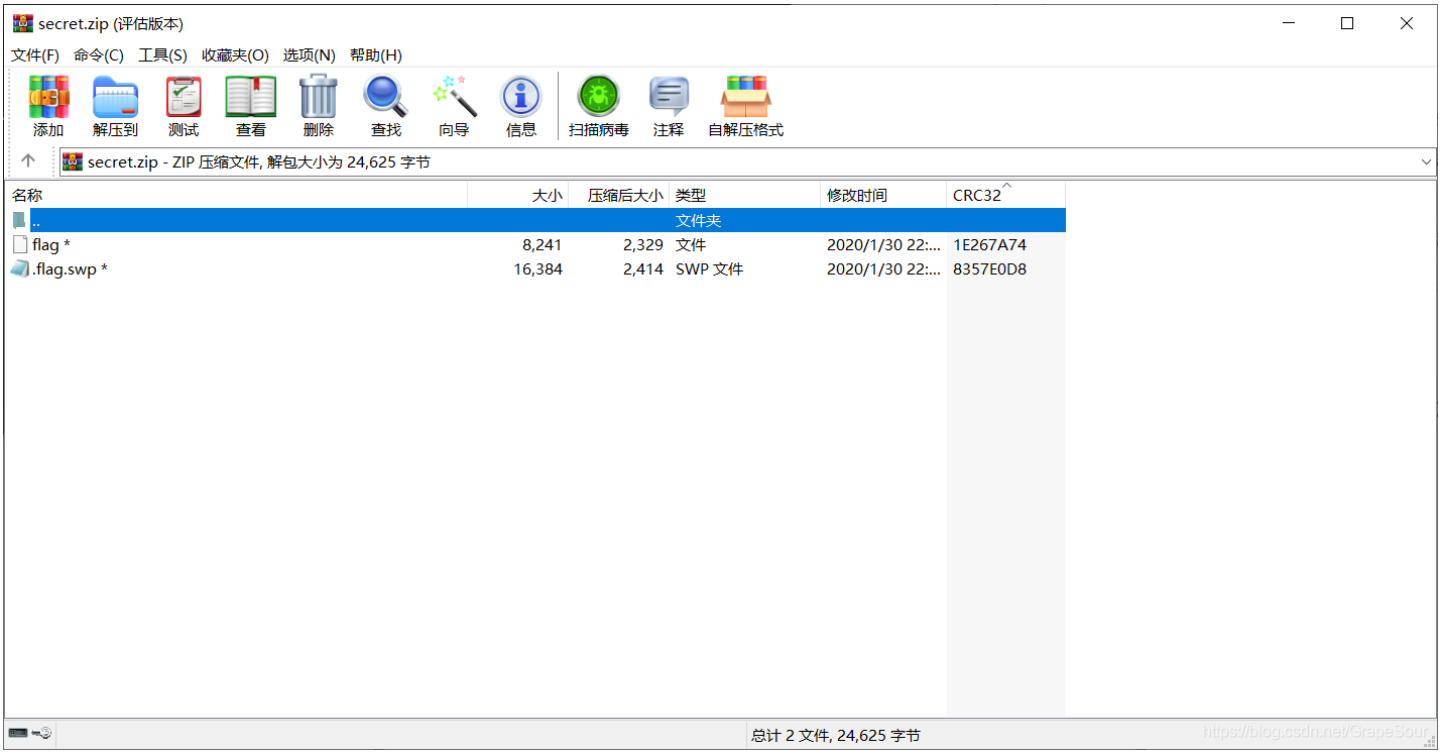

## [ACTF新生赛2020]swp

得到一个pcapng

http.request发现一个压缩包，有密码，因为没有什么思路就试试是不是伪加密，

```
.com          GET /a.gif?a=16ff7223b18&t=&i=2
com           GET /v.gif?logtype=0&title=%E6%
:81           GET /secret.zip HTTP/1.1
:81           GET /hint.html HTTP/1.1
:81           GET /favicon.ico HTTP/1.1
```

在将01改成00后



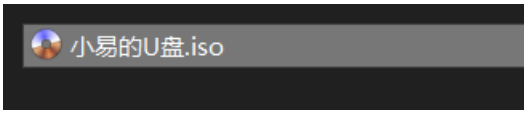

里面的swp文件可以提取出来了，得到flag

actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}

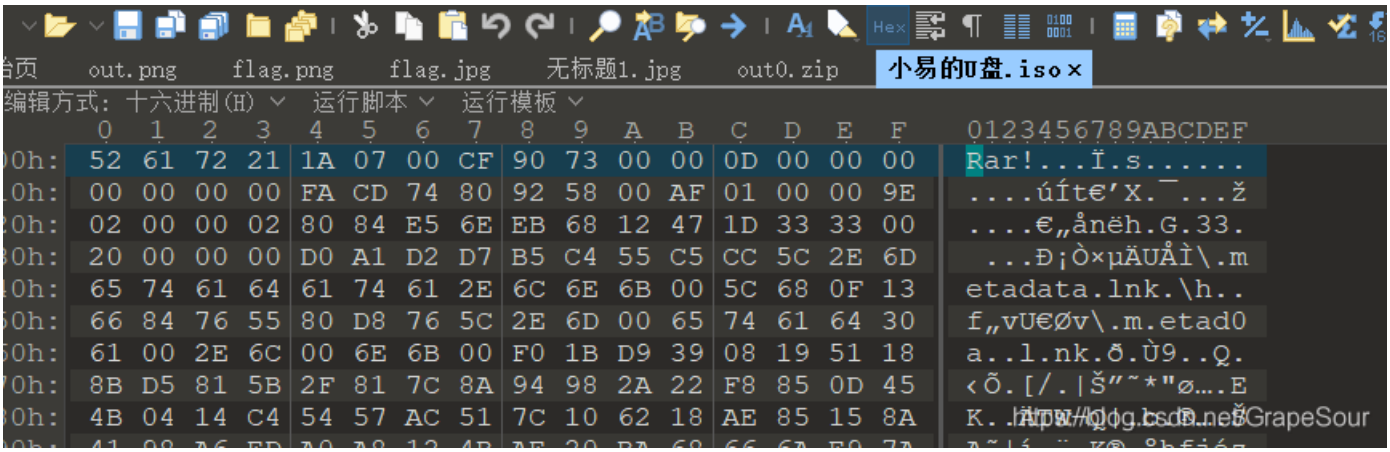
□□□:8

## 小易的U盘

得到




打开提示不是该文件类型，010打开发现是rar文件




修改后缀解压得到


用ida打开得到flag

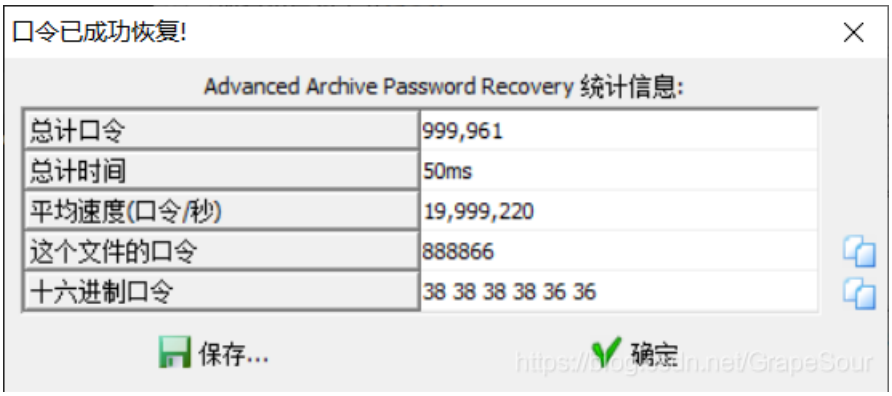
```
FILE *
crlek ; "flag{29a0vkrlek3eu10ue89yug9y4r0wdu10}"

FILE *
```

## 从娃娃抓起

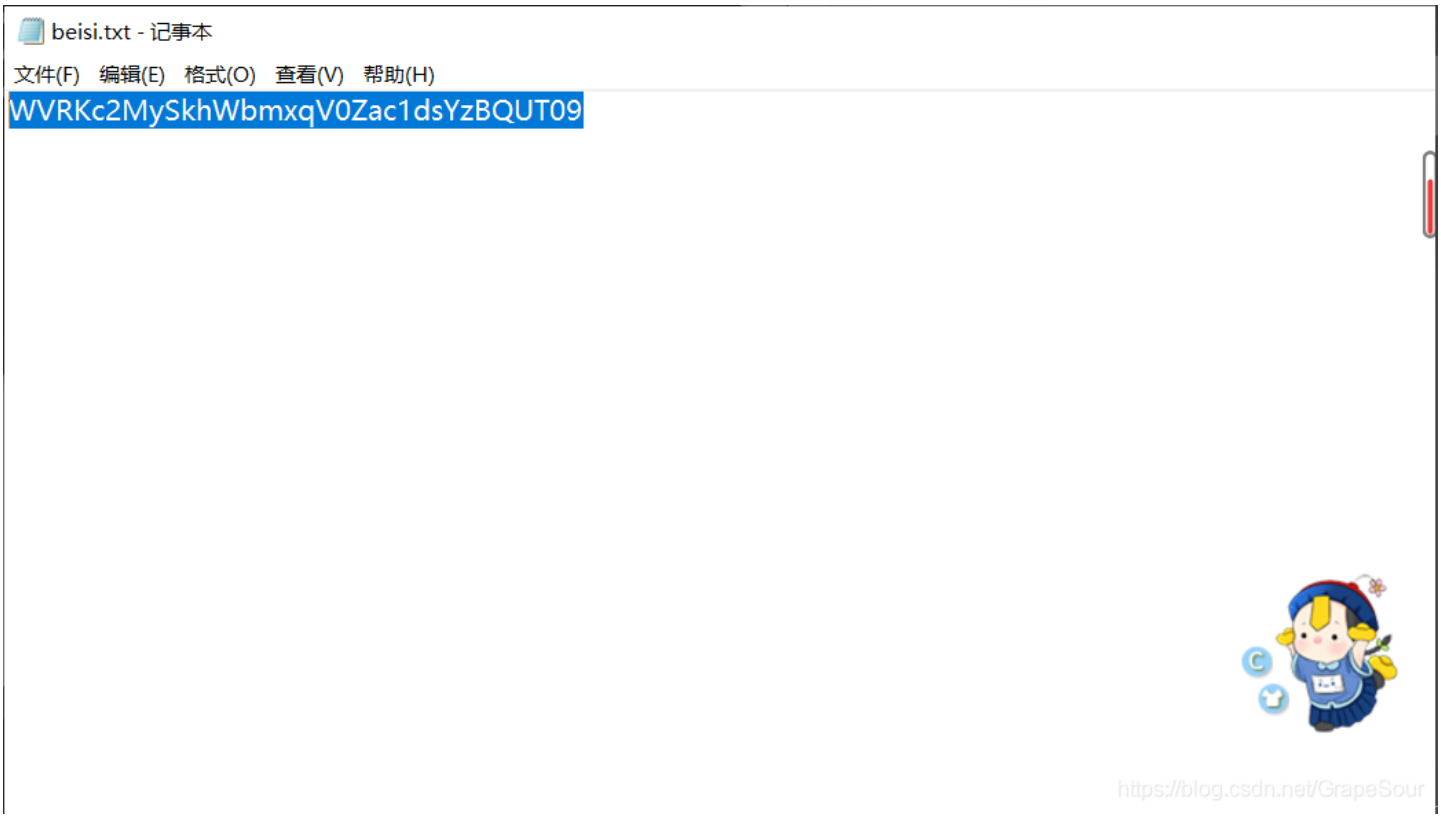
```
0086   1562   2535   5174            中文电码
 人      工      智      能
bnhn s wwy vffg vffg rrhy fhnv       五笔编码
也    要 从    娃    娃    抓    起

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}
```

## [WUSTCTF2020]alison_likes_jojo

打开，发现boki.jpg后有一个压缩包
提取出来，有密码先看第二个，看了半天没有什么头绪，爆破压缩包试试




得到密码




多次解密得到


没有头绪，查wp发现是outguess隐写，得到flag


## [DDCTF2018](ノ°□°)ノ ┻━┻

按照每两位截取

```
['d4', 'e8', 'e1', 'f4', 'a0', 'f7', 'e1', 'f3', 'a0', 'e6', 'e1', 'f3', 'f4', 'a1', 'a0', 'd4', 'e8', 'e5', 'a0
', 'e6', 'ec', 'e1', 'e7', 'a0', 'e9', 'f3', 'ba', 'a0', 'c4', 'c4', 'c3', 'd4', 'c6', 'fb', 'b9', 'b2', 'b2', '
e1', 'e2', 'b9', 'b9', 'b7', 'b4', 'e1', 'b4', 'b7', 'e3', 'e4', 'b3', 'b2', 'b2', 'e3', 'e6', 'b4', 'b3', 'e2',
 'b5', 'b0', 'b6', 'b1', 'b0', 'e6', 'e1', 'e5', 'e1', 'b5', 'fd']
```

转成10进制

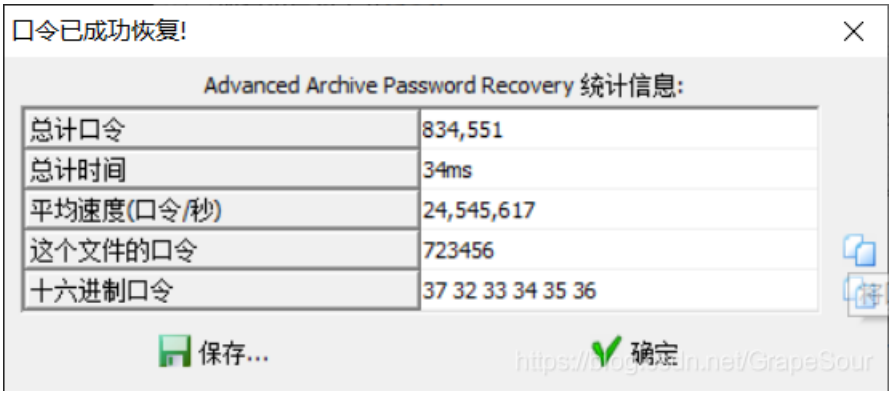
```
[212, 232, 225, 244, 160, 247, 225, 243, 160, 230, 225, 243, 244, 161, 160, 212, 232, 229, 160, 230, 236, 225, 2
31, 160, 233, 243, 186, 160, 196, 196, 195, 212, 198, 251, 185, 178, 178, 225, 226, 185, 185, 183, 180, 225, 180
, 183, 227, 228, 179, 178, 178, 227, 230, 180, 179, 226, 181, 176, 182, 177, 176, 230, 225, 229, 225, 181, 253]
```

每个减128
再转成字符串，得到flag

```
That was fast! The flag is: DDCTF{922ab9974a47cd322cf43b50610faea5}
```

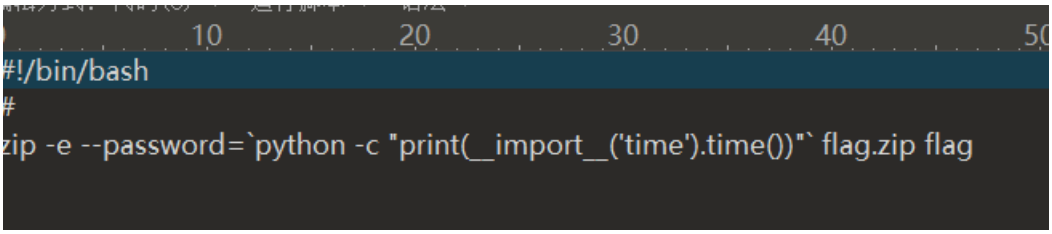
## [GUET-CTF2019]zips

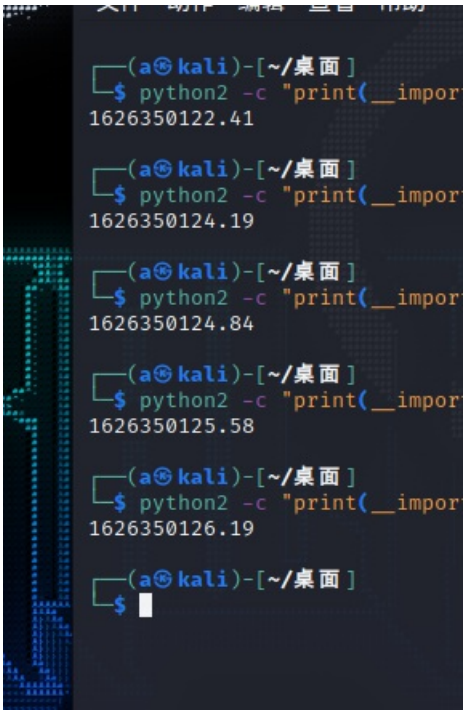
解压得到一个压缩包
爆破得到密码




又得到一个加密zip

111.zip是伪加密，解压后得到两个
setup.sh里面是这个，在kali里面执行一下试试




这里是以时间戳作为压缩包的密码，但是出题的时候的时间戳肯定和现在不一样，估摸一下确定时间戳前两位为15

使用ARCHPR掩码爆破，设置掩码15???.??，掩码符号?