杂项题目练习（二）

前言：

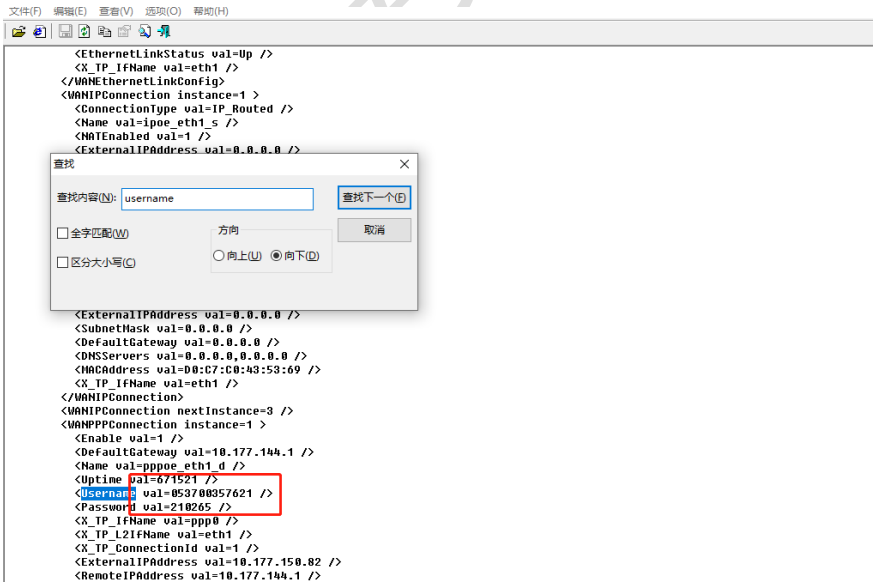
以下是我在 bugku 练习的解题思路，编号跟我前面分享的基础是对应的，理论基础结合实践。

所有题目目录如下：

以下是对 9-17 题的介绍

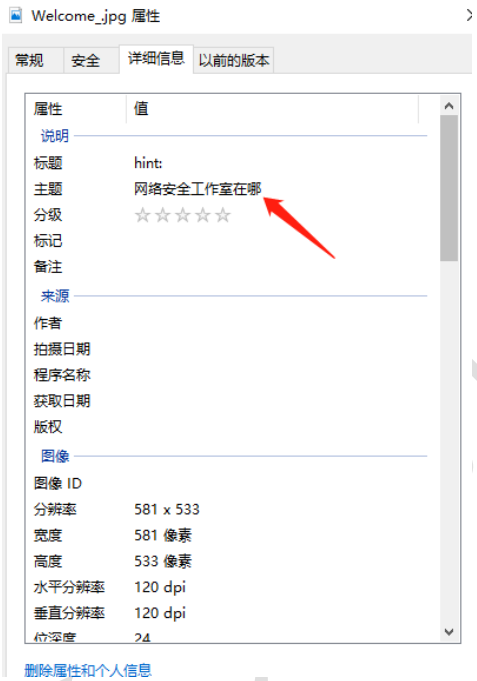
杂项第九题：宽带信息泄露

下载 bin 文件
打开题目，得到一个 bin 文件
名字是 conf
根据题目提示
使用工具 RouterPassView 打开这个文件（为什么使用这个工具请百度这个工具的作用信息）
搜索 username
得到 flag



杂项第十题：隐写 2

图片到本地
查看图片属性，看到有 hint



“网络安全工作室在哪”不知道这个啥意思。
用 UE 打开看到了很多 00 填充数据，怀疑是捆绑了文件在里面。
binwalk 分析一下

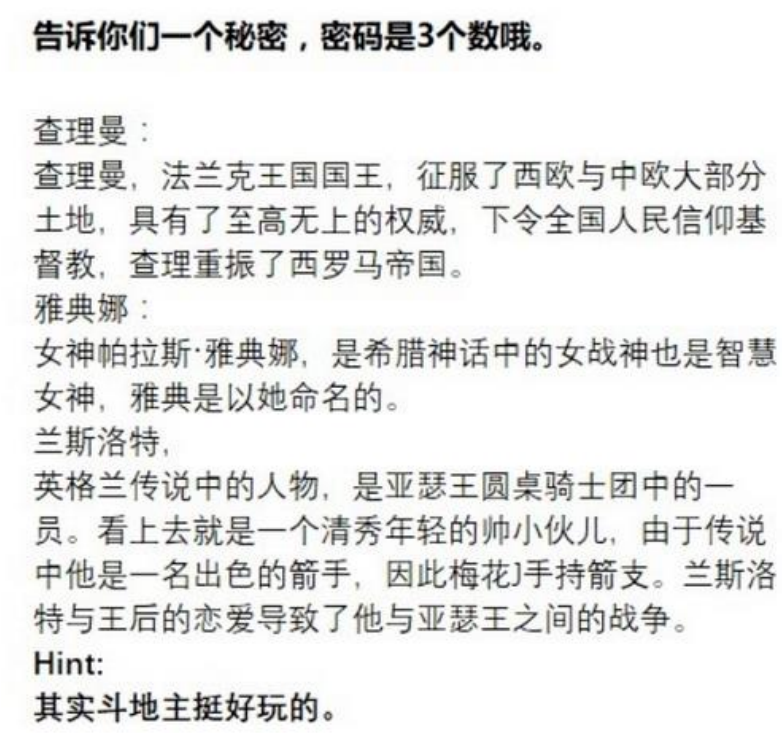
```
root@LAPTOP-OQE1H5K9:~/Desktop# binwalk -e 1.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
4444          0x115C          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc=
"http://p
4900          0x1324          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:li xml:lang="x-default">hint:</rdf:li></rdf:Alt>
52516         0xCD24          Zip archive data, at least v1.0 to extract, compre
ssed size: 6732, uncompressed size: 6732, name: flag.rar
59264         0xE780          End of Zip archive
147852        0x2418C         End of Zip archive
```

果然内含 zip 文件。用 dd 命令提取。
dd if=1.jpg of=2.zip skip=52516 bs=1

```
root@LAPTOP-OQE1H5K9:~/Desktop# dd if=1.jpg of=2.zip skip=52516 bs=1
95358+0 records in
95358+0 records out
95358 bytes (95 kB, 93 KiB) copied, 0.221955 s, 430 kB/s
```

解压 2.zip 之后有两个文件。

看了一下提示。



看了半天。。不想烧脑了。反正 flag.rar 的密码是三位数。直接暴力破解就好了。

```
root@LAPTOP-OQE1H5K9:~/Desktop# file flag.rar
flag.rar: Zip archive data, at least v2.0 to extract
```

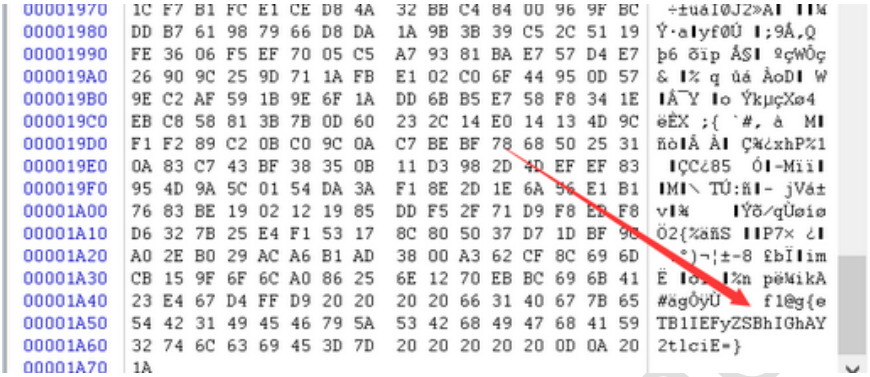
这里被后缀名套路了，一开始以为是 rar 压缩包，用 rar 的破解工具提示格式不正确。然后用 file 命令一检查，发现是 zip 压缩文件。
fcrackzip -b -l 3-3 -c1 -v flag.zip
放到 Kali Linux 中用 fcrackzip 工具破解。

```
root@LAPTOP-OQE1H5K9:~/Desktop# fcrackzip -b -l 3-3 -c1 -v flag.zip
found file '3.jpg', (size cp/uc   6588/  6769, flags 801, chk 102c)
possible pw found: 035 ()
possible pw found: 337 ()
possible pw found: 728 ()
possible pw found: 871 ()
```

解出来密码是 871。解压 flag.zip

3.jpg

然后又是一副图片。用 UE 打开查看文件头尾。
在文件尾处发现 flag。



f1@g{eTB1IEFyZSBhIGhAY2tlciE=}

但是一提交又不对，猜测是因为需要 Base64 解码里面的内容

f1@g{y0u Are a h@cker!}

杂项第十一题：多种方法解决

打开链接，下载压缩包：http://123.206.87.240:8002/misc/3.zip
解压后得到一个 exe
下载附件，解压 ，发现是 exe 文件，然后兴致冲冲的跑去 Windows7 x64 下运行，报错，然后又去 Windows7 x86 下运行，报错。

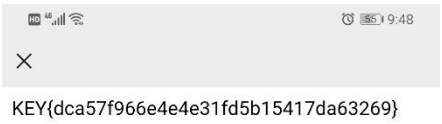
是我太年轻，这个 exe 文件没这么简单。

notepad 查看下文件，发现应该是一张图片，但是进行了 base64 编码。

```

QU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hw
PCDcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rXO3P4lLvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78zhU+5i9yxv
4T3T2O0/7eud68OT2H3LCft0l/ae9Z1To+23pPvX7/rwJHbfcsI+3aW9Z33mlGj7Len+9bs+PIndt5ywT3dp7lmfOT
Xafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S7l+/68MJc5O0OSWpcyexnFjfcsI+JWlukpRfv+vDCXOTtDklqXMnsZxY
33LCPiVtbpKUX7/rwwlzk7Q5JalzJ7GcWN9ywj4lbW6S1F+/68MJc5O0OSWpcyexnFjfcsI+JWlukpRfv+vDCXOTWE
7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73PctL2DbvH3CQpv37XhxPm
JrGctPld7H2Wk7Zv2D3mJkn59bs+nDA3ieWEfdNImylJnelp7H6bmyTll+/6cMLcJJYT9k0jbaYkdaansfttbpKUX7
/rwwlzklhO2DeNtJmSlJmexu63uUlSfv2uDyfMTWI5Yd800mZKUmd6Grvf5iZJ+fW7PjzJ7vl2b33LSdtvsfuW75Lu
X7/rw5Ps3m/3lrectP0Wu2/5Lun+9bs+PMnu/XZvfctJ22+x+5bvku5fv+vDk+zeb/fWt5y0/Ra7b/ku6f71+++HT0
v+5l3+tK935vApyd+8y5/29c4cPiX5m3f5077emcOnJH/zLn/ar3d+/flBpI+cMDeNtJkSywn79BP5uK+yfzTmppE2
U2I5YZ9+Ih/3VfaPxtw00mZKLCfs00/k477K/tGYm0baTInlhH36iSxflT78TpI605bdPbF7lhvct54mvW0aWJ6m4Z
0kdaYtu3ti9yw3uG89TXrHNLE8TcM7SepMW3b3xO5ZbnDfepr0jmlieZqGd5LUmbbs7onds9zgvvU06R3TxPXcSxPr
W07YpyRlpqTNKUmdKUmdk5LUaXzdWB/eYX3LCfuUpM6UtDklqTMlqXNSkjqNrxvrwzusbzlhn5LUmZI2pyRlpiRlTk
pSp/FlY3l4h/UtJ+xTkjpT0uaUpM6UpM5JSeo0ft34+vOGNLqDfUosN7inhvUtJ+ybRtpMd0n39Goa3cE+JZYb3FPD
+pYT9k0jbaa7pHt6NY3uYJ8Syw3uqWF9ywn7ppE2013SPb2aRnewT4nlBvfUsL7lhH3TSJvpLunecjWV7mCftqQbjS
RlpuR03tqSbkx/wrJqj7JPW9KNRpI6U3I6b2lJN6Y/YVmlR9mnLelGI0mdKTmdt7akG9OfsKzao+zTlnSjkaTOlJzO
WlvSjelPWFbp8NRImylJnWnL7r6F7zN3STcb32FppUNTI22mJHWmLbv7Fr7P3CXdbHyHpZUOTY20mZLUmbbs7lv4Pn
OXdLPxHZZWOjQl0mZKUmfasrtv4fvMXdLNxndYWunQlFhutHv2W42n+4bds7wl3VuuskSJ5Ua7Z7/VeLpv2D3LW9K9
5SpLlFhutHv2W42n+4bds7wl3VuuskSJ5Ua7Z7/VeLpv2D3LW9K97avp6GQ334X3KWlz+tukb5j+hO2/hX3Ebr4L71
PS5vS3Sd8w/Qnbfwv7iNl8F96npM3pb5O+YfoTtv8W9hG7+S68T0mb098mfcP0Jxz/W+x+FPethvUtN2y/m7fwnvml
+frzIOklDdy3Gta33LD9bt7Ce+bX5uvPg6SXNHDfaljfcsP2u3kL75lfm68/D5Je0sB9q2F9yw3b7+YtvGd+bb7+vC
EN7ySpMzXSZrqL3bOcsN9Kns4T2uJRk6TOlEib6S52z3LCfit50k9oi0dNkjpTI22mu9g9ywn7reTpPKEtHjVJ6kyN
tJnuYvcsJ+y3kqfzxNLiEUosJ+xTYvkudt9yg3tqpM2d5Cf50mKJEssJ+5RYovodt9zgnhppcyf5Sb60WKLEcsI+JZ
bvYvctN7inRtrcSX6SLy2WKLGcsE+J5bvYfcsN7qmRNneSn+RLK5UmbW4Sywn7lOzmhH3a0u7ZN99hadmRNjeJ5YR9
SnZzwj5taffsm++wtOxIm5vEcsI+Jbs5YZ+2tHv2zXdYWnakzUliOWGfkt2csE9b2j375jtcvTz+tuX0vrXF9sxNkj
rTT+T6rvyx37ac3re22J65SVJn+olc35U/9tuW0/vWFtszN0nqTD+R67vyx37bcnrf2mJ75iZJneknUn+V/aWYUyNt
pqTNqZE2UyNtGlvSjTsT9VvtKHNqpM2UtDk10mZqpEljS7pxZ6J+qxllTo20mZI2p0baTI20aWxJN+5MlG+1o8ypkT
ZT0ubUSJupkTaNLenGnYnl6TujO2zP3DTSZkp2c8L+0xppM32HpfWTIxPbMzeNtJmS3Zyw/7RG2kzfYWn95MjE9sxN
I22mZDcn7D+tkTbTdlhaPzkysTlz00ibKdnNCftPa6TN9B2uXh5/S9rcbEk37jR2+5SkzpSkzo4kdaavTg6/JWlutq
Qbdxq7fUpSZ0pSZ0eSOtNXJ4ffkjY3W9KNO43dPiWpMyWpsyNJnemrk8NvSZubLenGncZun5LUmZLU2ZGkzvTVWR/e
0faJ7Xdzw/bMKbGc7PbNElx3uqNtn9h+Nzdsz5wSy8lu3zzBdac72vaJ7Xdzw/bMKbGc7PbNElx3uqNtn9h+Nzdsz5
wSy8lu3zzBcsVewpySlLmTWG7Y3nLCPmlJN05KLP/D8tRGzClJnTuJ5YbtLSfs05Z046TE8j8sT23EnJLUuZNYbtje
csI+bUk3Tkos/8PylEbMKUmdO4nlhu0tJ+zTlnTjpMTyP/R/i8PwI//fJZYb3Jvv8Pd/il+WWG5wb77D3/8pflliuc
G9+Q5//6f4ZYnlBvfmOly9PH7KFttbfhq+zySpMyVtbr7Dlcvjp2yxveWn4ftMkjpT0ubmOly9PH7KFttbfhq+zySp
MyVtbr7Dlcvjp2yxveWn4ftMkjpT0ubmOly9ftRq9v0n7FPD+paTtk9O71sTl3Mv7WD3LSfsU8P6lpO2T07vWxPXcv
```

于是，在线转码啦 ~
http://tool.chinaz.com/tools/imgtobase/
全选 复制 notepad 中内容到在线转码中

扫描二维码得 flag



KEY{dca57f966e4e4e31fd5b15417da63269}

KEY{dca57f966e4e4e31fd5b15417da63269}

杂项第十二题:闪的好快

打开图片是个一直闪的二维码
这是一道二维码的题目。
保存图片祭出神器 StegSolve。

然后 Analysis->Frame Browser

Frame Browser：帧浏览器，主要是对 GIF 之类的动图进行分解，动图变成一张张图片，便于查看。

这里发现是 18 张图。也就是 18 张图片。

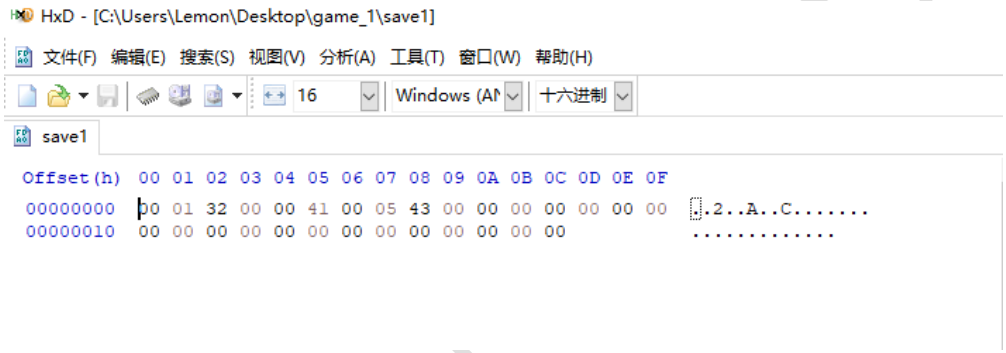
我拿手机一个挨着一个扫的。
扫出来的结果是 SYC{F1aSh-so-f4sT}
但是提交不正确。
最后更改为 SYC{F1aSh_so_f4sT}
60 分到手

杂项第十三题: come_game

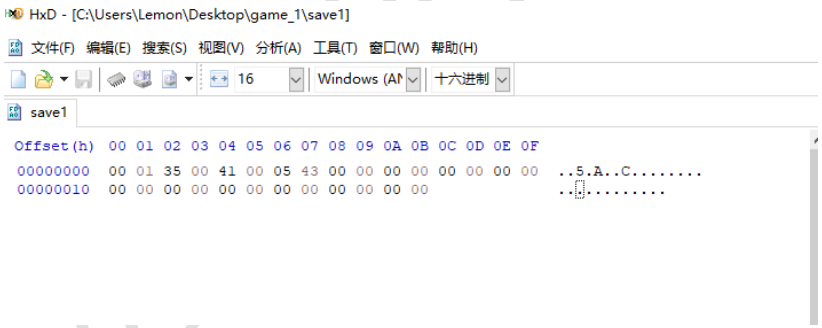
下载压缩包
打开后是个游戏

随便玩一玩，然后就发现生成了三个文件，一个 save

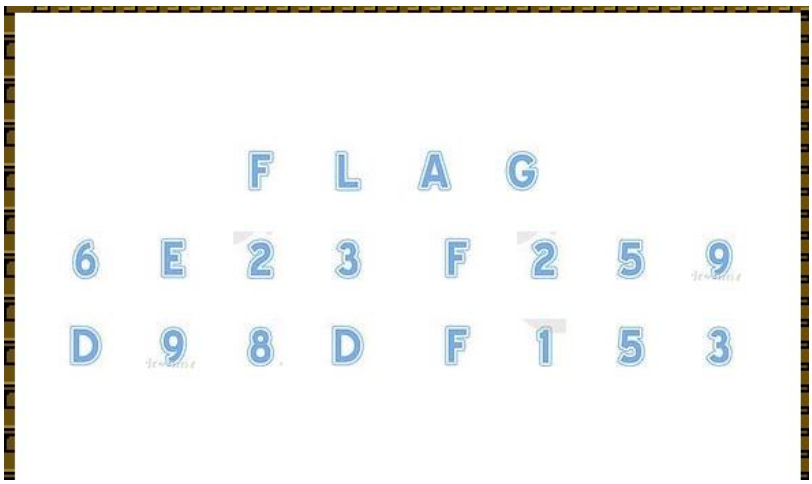
用 HXD 分析了下



然后发现这里 2 就是代表关卡的意思。我们这里修改成 5 也就是对应的 35



然后保存下，重新运行程序就出来 flag



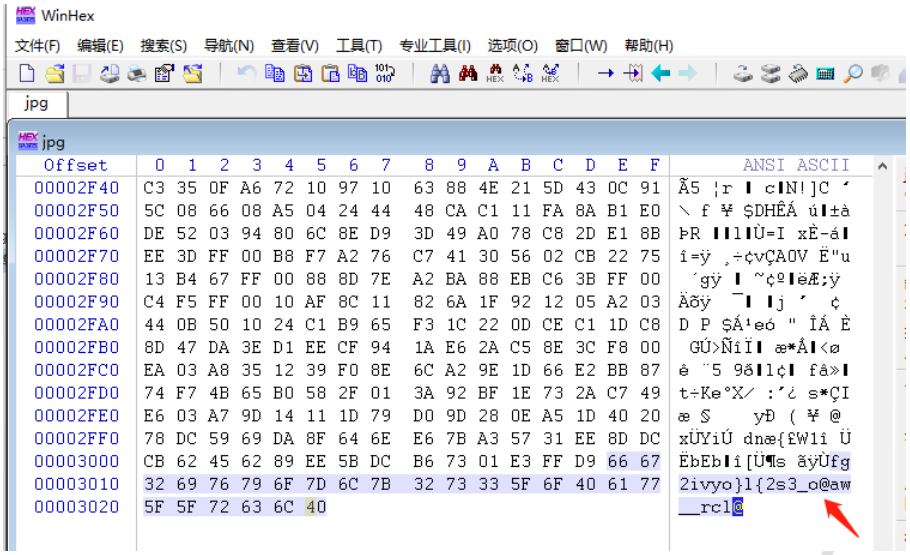
Flag{6E23F259D98DF153}
提交之后没有成功，不知道原因，但是看了大佬之后发现。
SYC{6E23F259D98DF153}，原来是格式有问题。

杂项第十四题：白哥的鸽子

下载图片

在 linux 中可以打开说明，宽高都没有修改。

扔进 winhex 中，只感觉结尾处有点奇怪



出现 flag 的样本，但是我不知道这是怎么处理，看了别人的解答，发现是栅栏密码：

```
# 3 个字符一组，一共 24 个字符，总共 8 组
str = "fg2ivyo}l{2s3_o@aw__rcl@"
flag = ""
for i in range(0, int(len(str)/3), 1):
    flag += str[i]
    flag += str[i + 8]
    flag += str[i + 16]
print(flag)
```

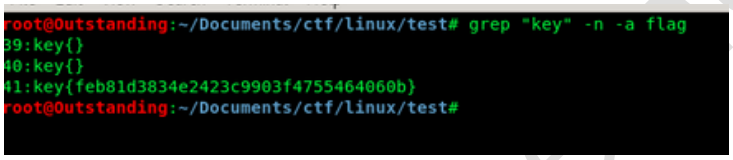
运行结果如下，两个@好像是干扰，直接去掉就行了 ：

flag{w22_is_v3ry_cool}@@
也可以用在线解密

杂项第十五题: linux

下载压缩包，解压后是个 flag 文件

grep "key" -n -a flag

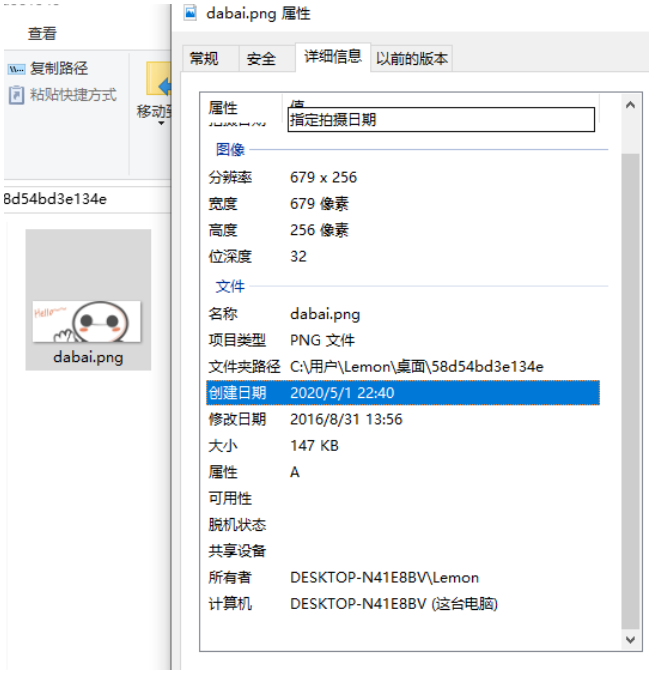


key{feb81d3834e2423c9903f4755464060b}

杂项第十六题: 隐写 3

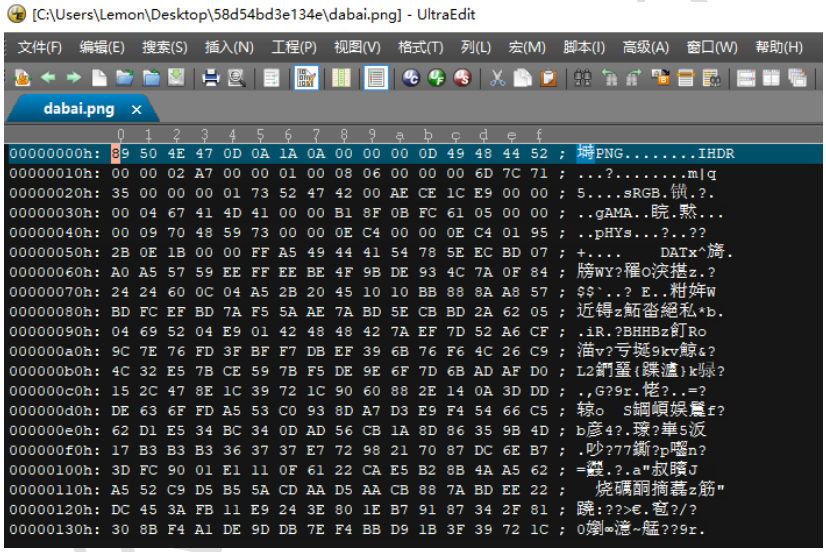
下载压缩包后解压 ， 解压后是个图片

根据提示隐写

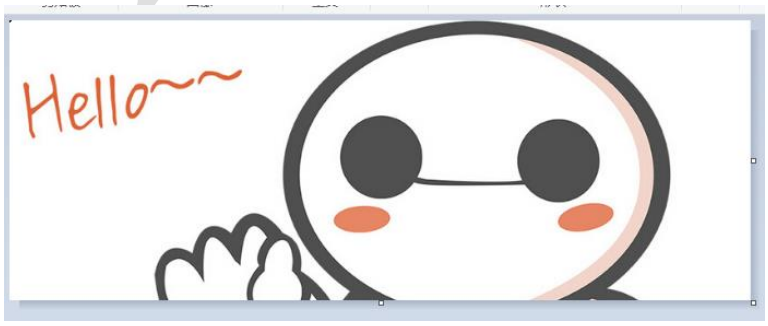


查看图片属性无发现

用 UE 查看图片

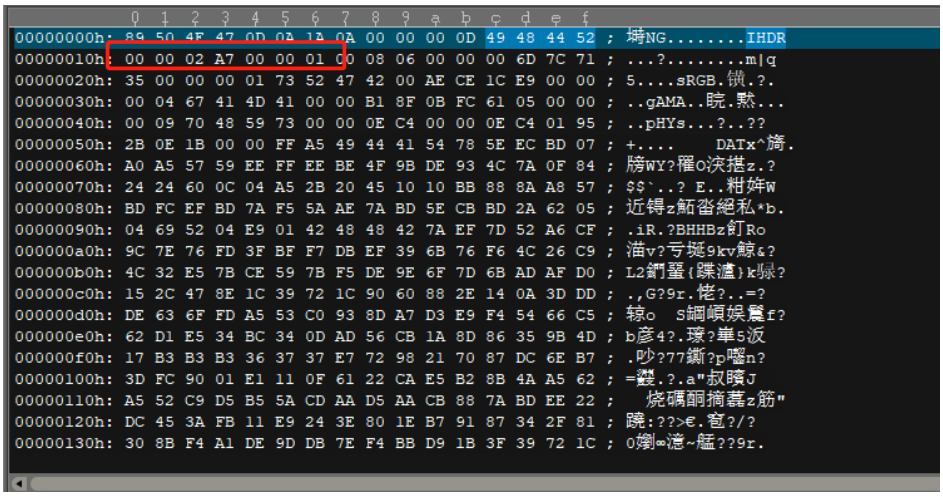


查看文件头文件尾，没有发现

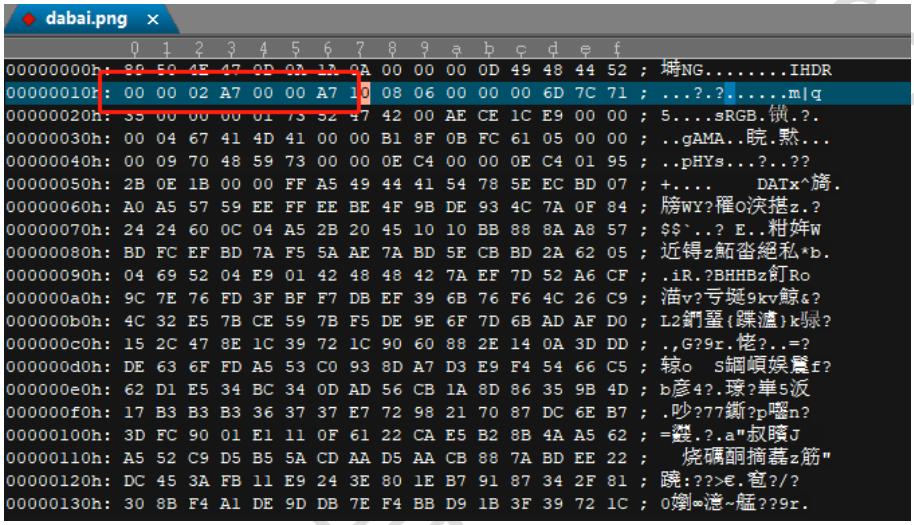


打开图片看高度和宽度，用 UE 修改高度试试

之前文章中写到，**在 UE 中找到 IHDR，在这后面的八个 bit 就是宽高的值**



然后试图把高改成和宽一样的值，即把 01 改成 A7.



Windows 再次打开

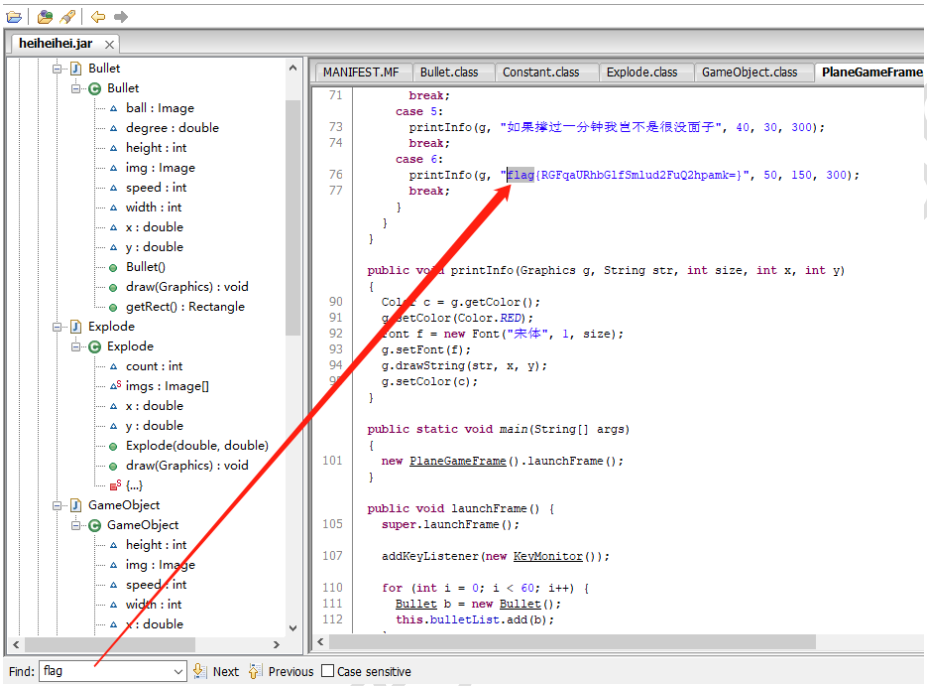
flag{He110_d4_ba1}

杂项第十七题：做个游戏(08067CTF)

下载 jar 文件
运行后是个动图

打开后，观察，题目说的坚持 60s，但是不知道是不是游戏的 Bug,我根本不知道怎么坚持 60s 就死了，所以此方法不可行。于是将文件拿到 jd-gui 下
用 jd-gui 分析代码

没有技巧性，只能一个文件一个文件的搜索



flag{RGFqaURhbGlfSmlud2FuQ2hpamk=}

提交报错。

一般看到{}中带有“=”的字样，一般为 base64 加密后的结果

因此，对此字符串进行 base64 解密，得到明文

BASE64 解密链接：https://base64.supfree.net/

flag{DajiDali_JinwanChiji}