

CTF——杂项WriteUp（题目1：代号）

原创

GreatYuTong 于 2020-03-16 22:06:46 发布 262 收藏 1

分类专栏: [CTF](#) 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/GreatYuTong/article/details/104907316>

版权



[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏



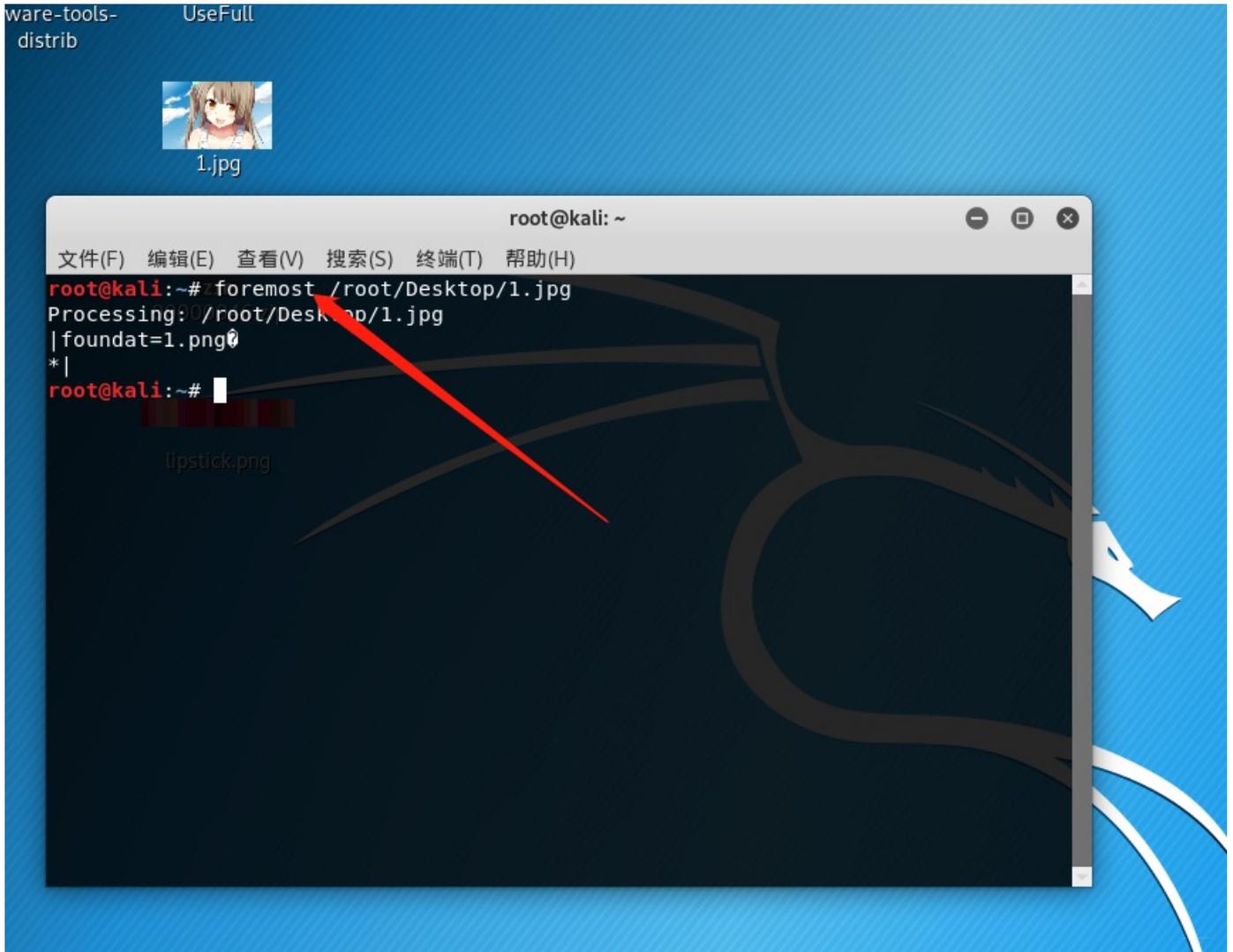
下载附件, 解压得一张照片, 看下图(叫“代号.jpg”):

看看照片上的妹妹, 是不是很可爱呢? 拿到图片, 我第一反应就是拖到记事本里面, 然后CTRL+f查看关键字“flag, key等”, 不过本题没有如何发现。

好吧, 那我们就copy到kali里面, 用binwalk命令查看图片都隐藏什么信息吧(原图被我重命名为1.jpg), 请看下图(图片里面内嵌有加密的zip文件):

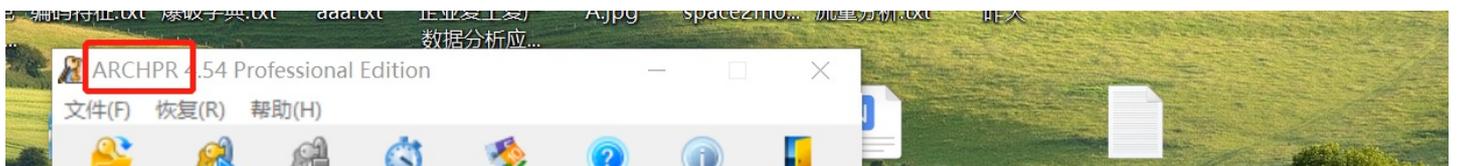
```
root@kali: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali:~# binwalk /root/Desktop/1.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0          JPEG image data, JFIF standard 1.01
23949       0x5D8D       Zip archive data, encrypted at least v2.0 to extract, compressed size: 194574, uncompressed size: 200059, name: 1.png
218683      0x3563B      End of Zip archive, footer length: 22
00000046.zip
```

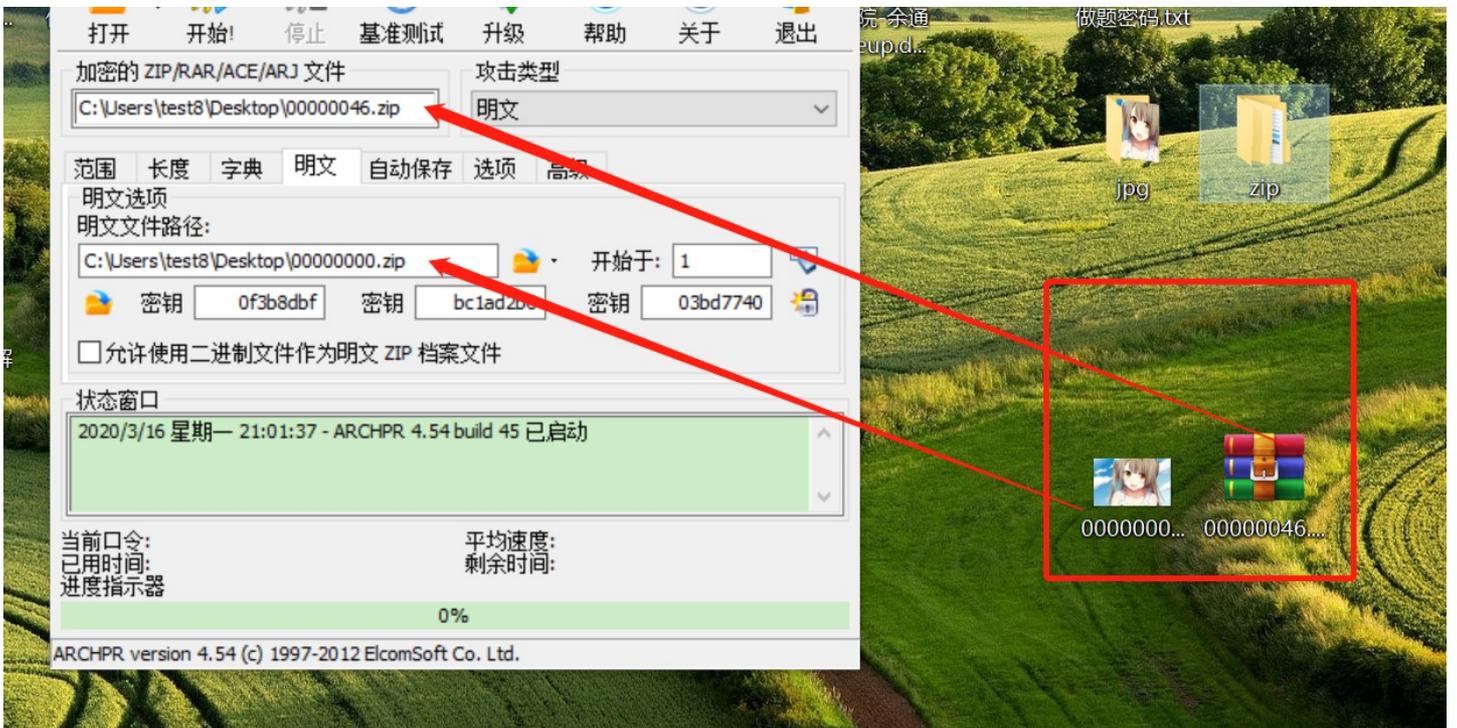
在命令行用foremost命令分离图片，（备注：执行命令前，先将主目录下的output文件夹下的内容清空）看下图：



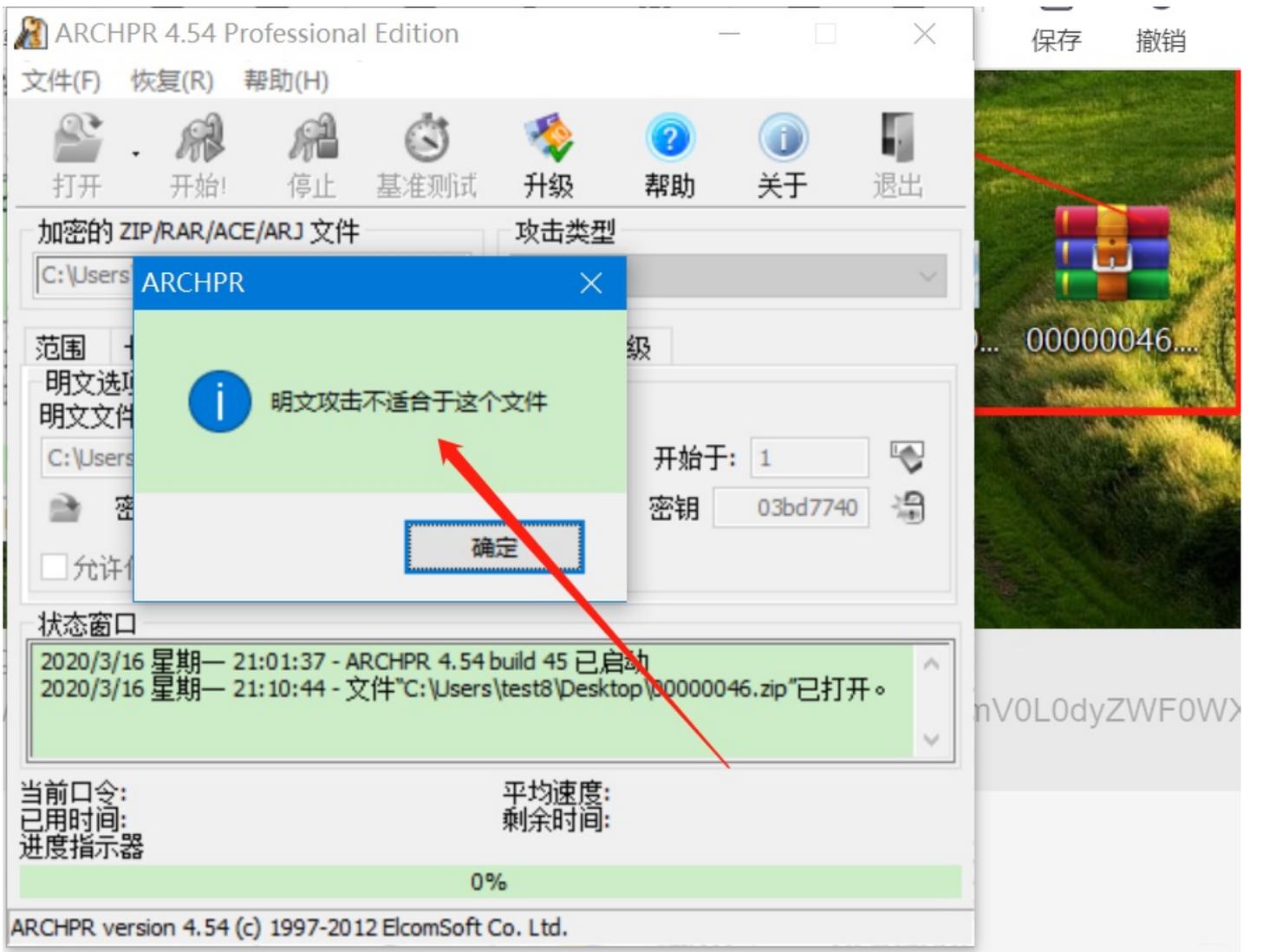
解压zip文件，确实是加密的，所以，接下来就是想法设法爆破密码了。

copy压缩包，回到物理主机，打开ARCHPR破解软件，然而我们首先想到的是明文攻击（因为同时分离出来一张照片0000000.png）将图片压缩，按下图操作，那就开始明文攻击吧！请看下图：

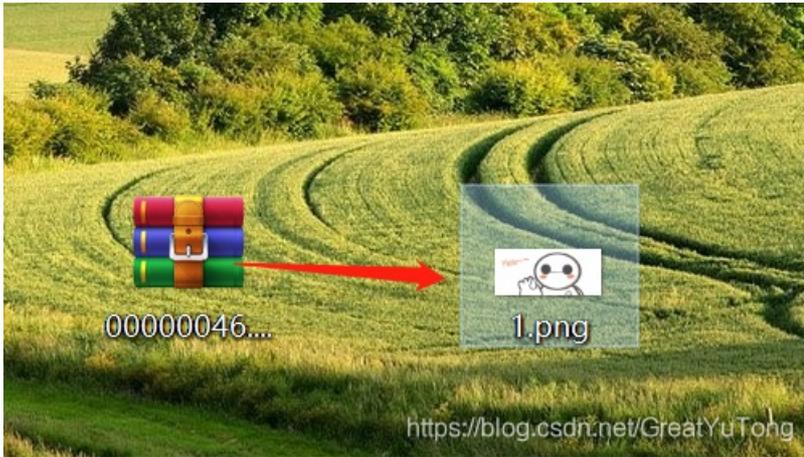
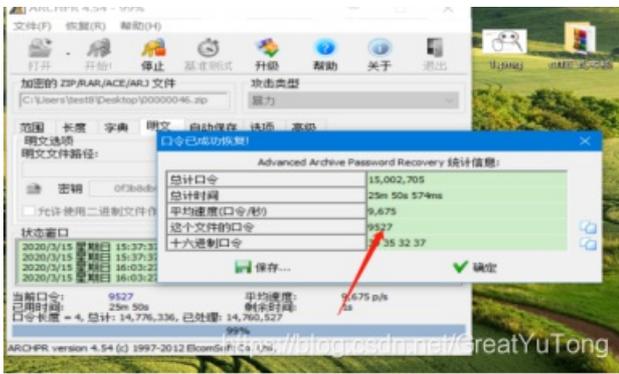




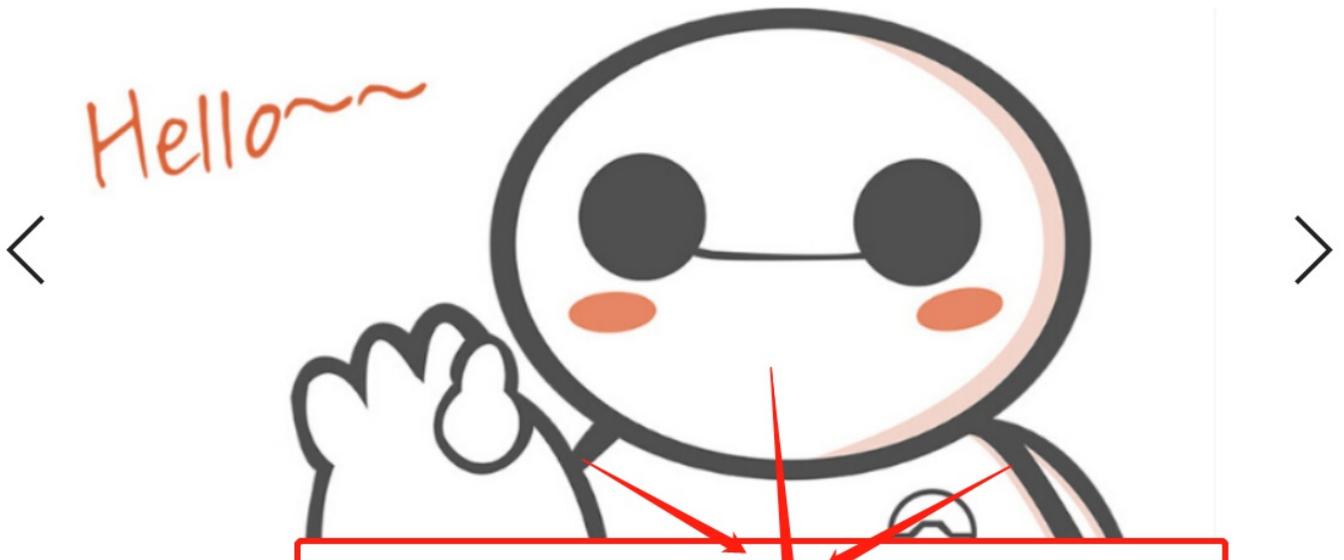
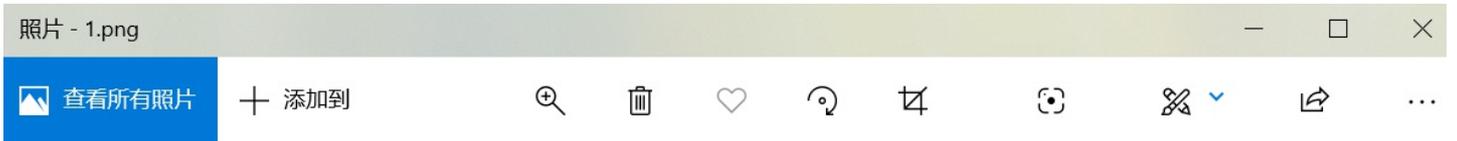
点击“开始”，我Cao，好像不行哦：无法进行明文攻击.请看下图：



那特么怎么搞呢？？？就只能暴力攻击了，那就暴力攻击吧，请看下图（得解压密码：9527）：

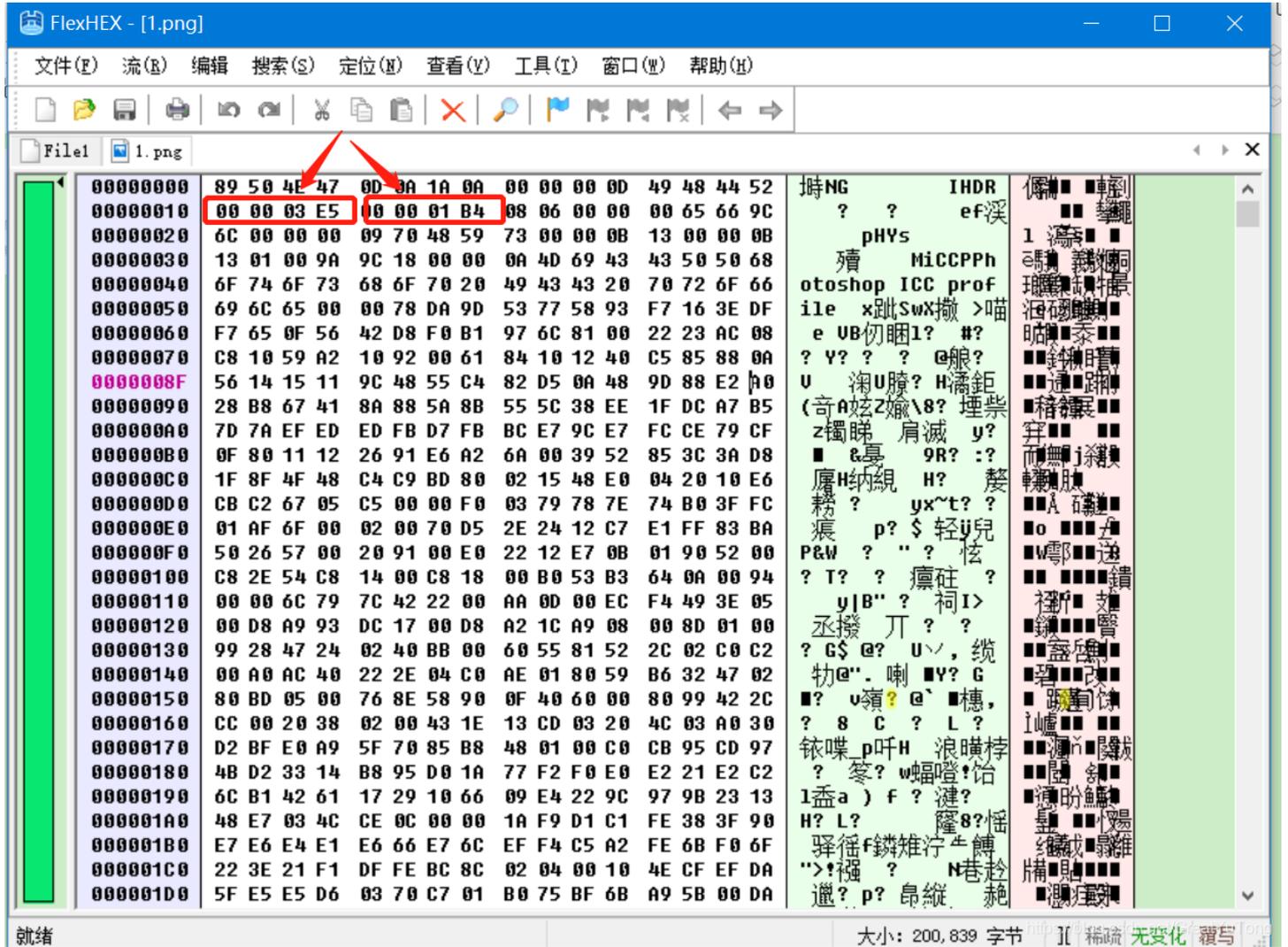


解压得1.png图片。打开图片看看吧，这张图片肯定是我们主攻的目标了，按我的习惯，还是托到记事本里面看看吧，发现没有什么异样的那就打开看看图片属性啥的，特么也是没有发现什么特殊的地方那！！！！！！我们再打开图片看看，请看下图：

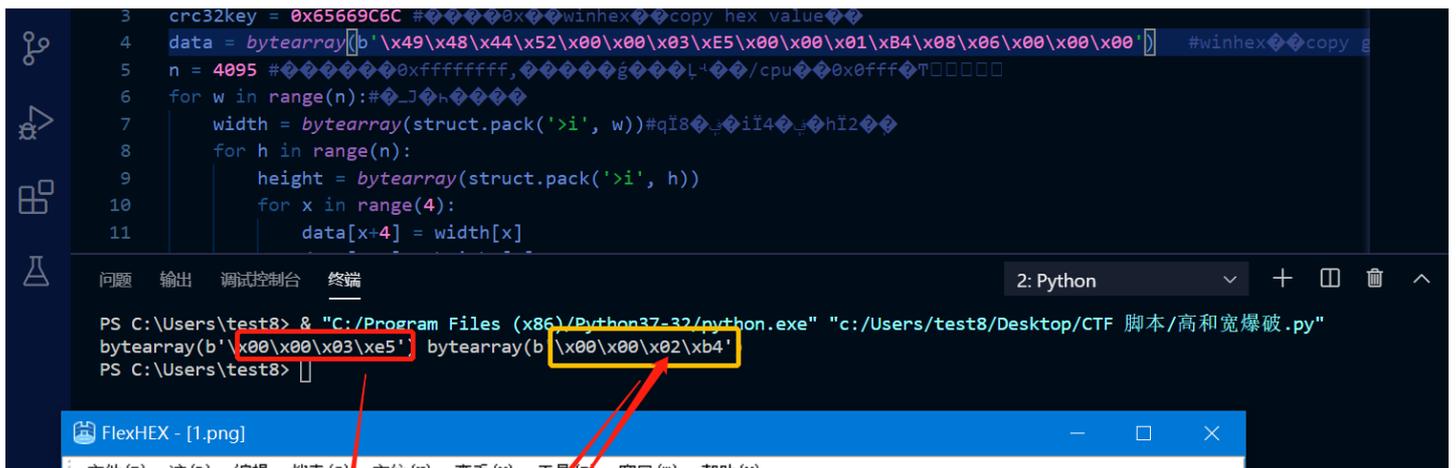


我们会发现图片不全呀!!! 图片的“下体”去哪里啦????? 第一感觉技术flag藏在MM的下面了——>那就是图片的宽高问题了...

好吧, 把图片放到FlexHEX中, 看看吧:

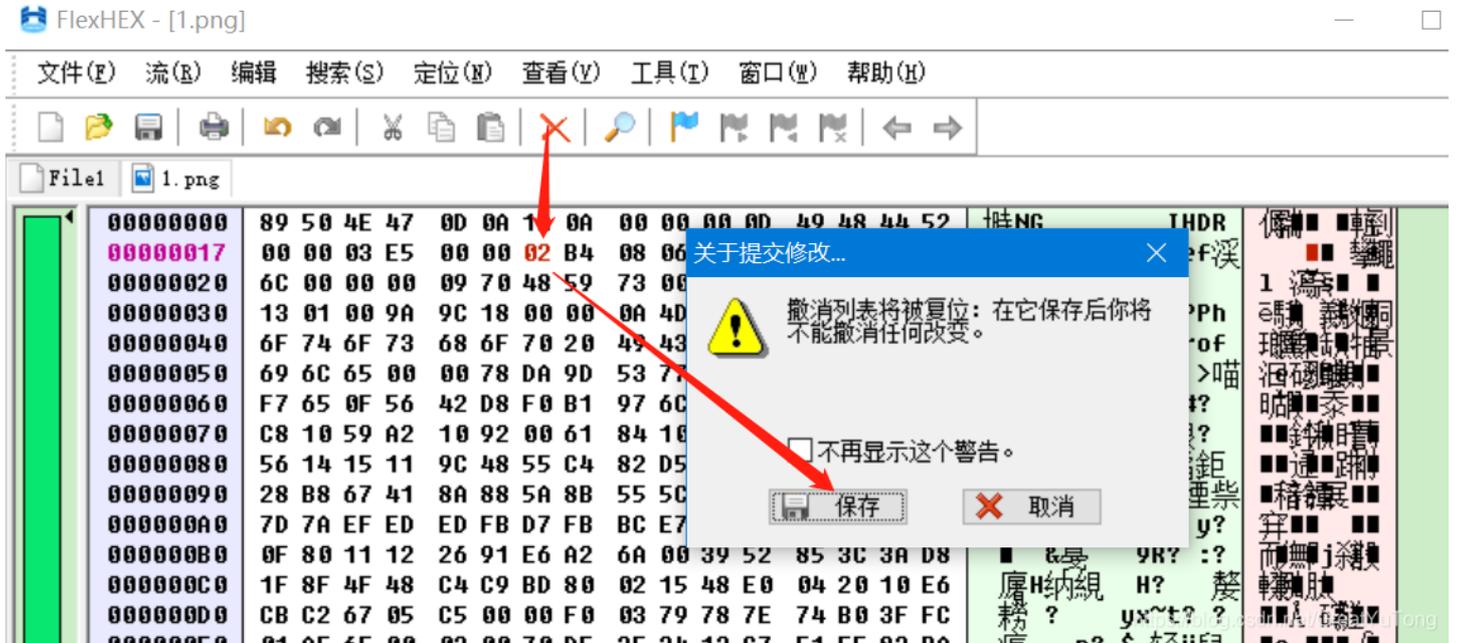


怎么改呢???? 也不能瞎几把改呀???? 那就是爆破了!!!! 好吧, 自己动手写个脚本开始爆破吧(也可以去网上下载), 请看下图:

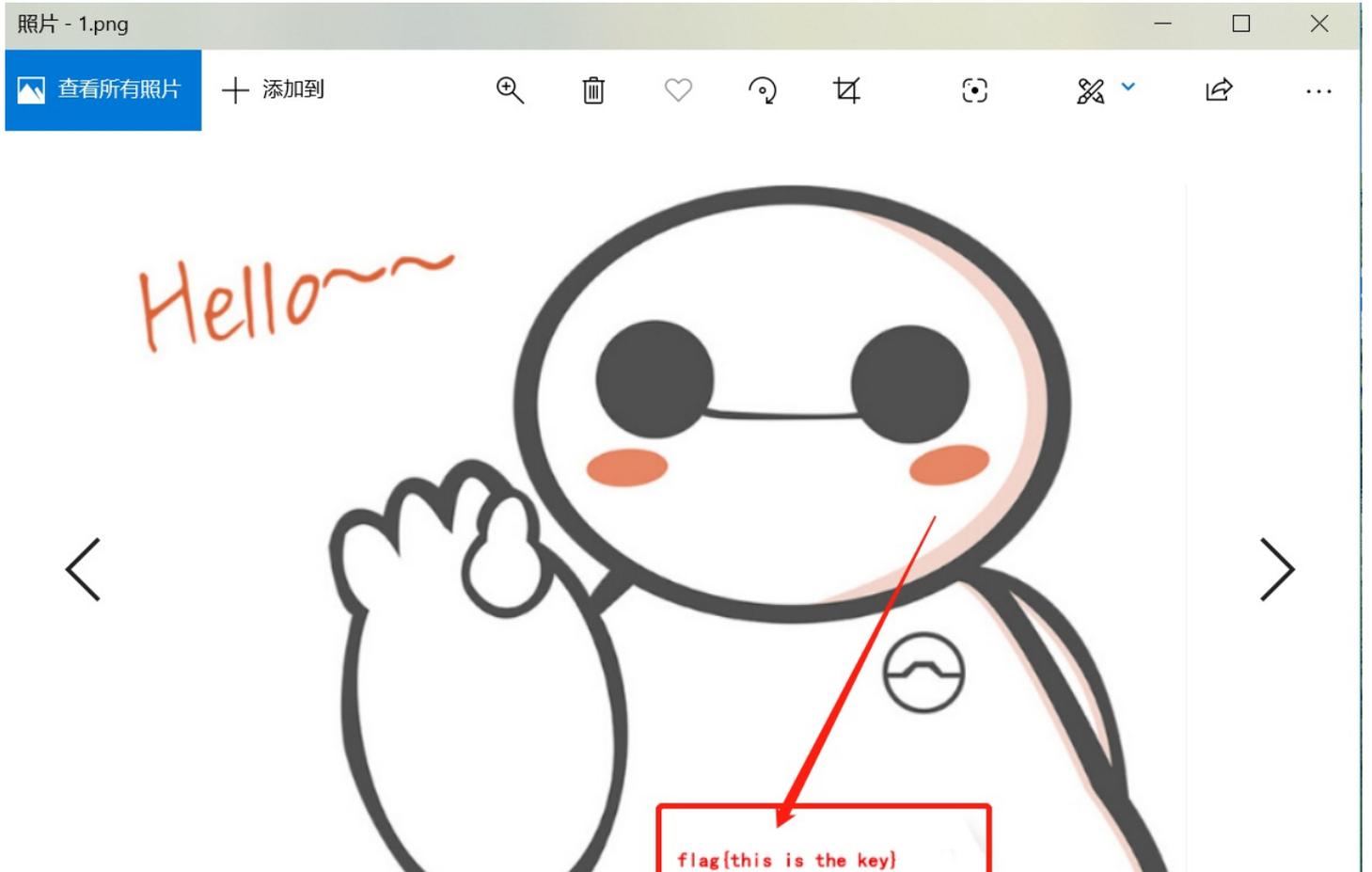




图中圈黄的部分，有何不同?? 所以把图片的高度中的01改为02，看下图：



保存，打开看看效果：



鸡动吗?????终于看到MM的下体的那个红色的flag了，接下来就识别图中的flag，复制提交既可。

本文属于原创，转载请说明出处。有问题的请留言！



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)