杂项题目练习（一）

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 1-8 题的介绍

通常做图片隐写的题，大概都是先右键查看属性，看下有没有一些特殊的信息，没有就放 binwalk 看下有没有隐藏什么文件，又或者直接 stegsolve 分析一波。

杂项第一题：签到题

就是签到题，关注后得 flag
flag{BugKu-Sec-pwn!}

杂项第二题：这是一张单纯的图片

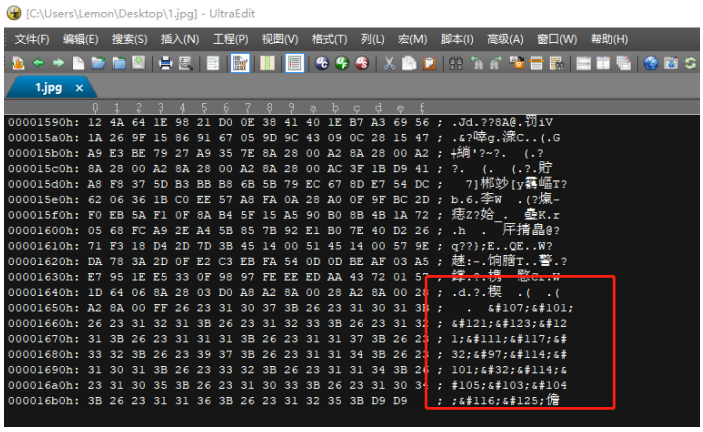
打开后

http://123.206.87.240:8002/misc/1.jpg

打开题目所给的链接，发现是一张图片，应该是考察隐写术。右击保存图片到本地。

先看了一眼文件属性，没有什么发现。。

然后用 UE 打开查看了下文件头部和文件尾部，在文件尾部发现 Unicode 编码，复制。



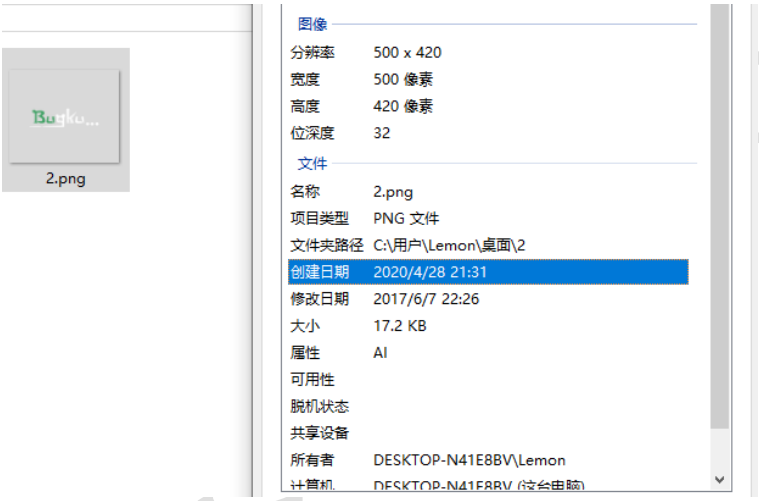
key{you are right}

解码：https://www.sojson.com/unicode.html

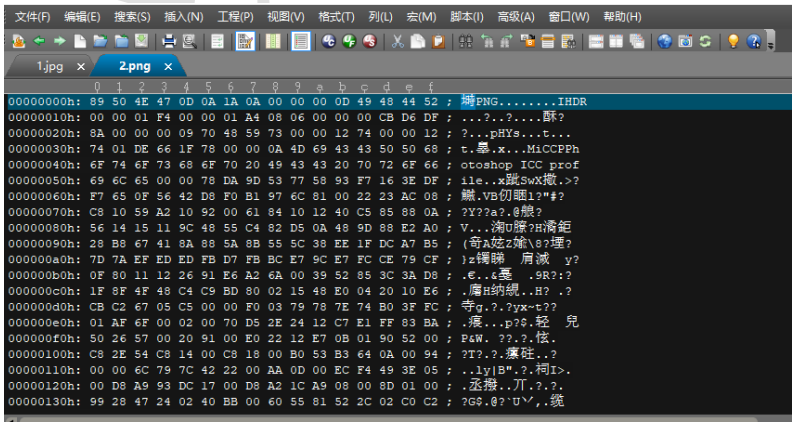
key{you are right}

杂项第三题：隐写

下载压缩包
解压出来一个图片
先看了一眼文件属性，没有什么发现。。



会发现一个神奇的现象就是缩略图不一样。怀疑是修改了 Exif 中的缩略图，但是图片后缀是 png 的先用 UE 打开查看下头文件判断一下是不是真的 png。一般来说 png 里不会嵌入 Exif 信息的。



89504E47 PE 头应该是 png 图片了。这样就排除了 Exif 的可能性，这个缩略图不一样可能是 ps 修改完之后没有更新缩略图信息造成的。看了下图片属性，无果。。用 UE 查看了下文件头尾，无果。。

之后想到修改图片宽高的方法还没尝试。

百度了一下 png 的文件格式

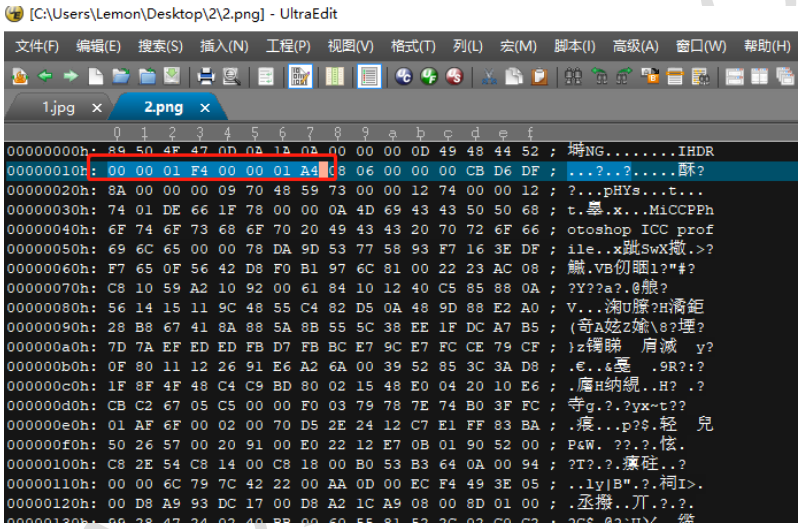
IHDR

文件头数据块IHDR(header　chunk)：它包含有PNG文件中存储的图像数据的基本信息，并要作为第一个数据块出现在PNG数据流中，而且一个PNG数据流中只能有一个文件头数据块。

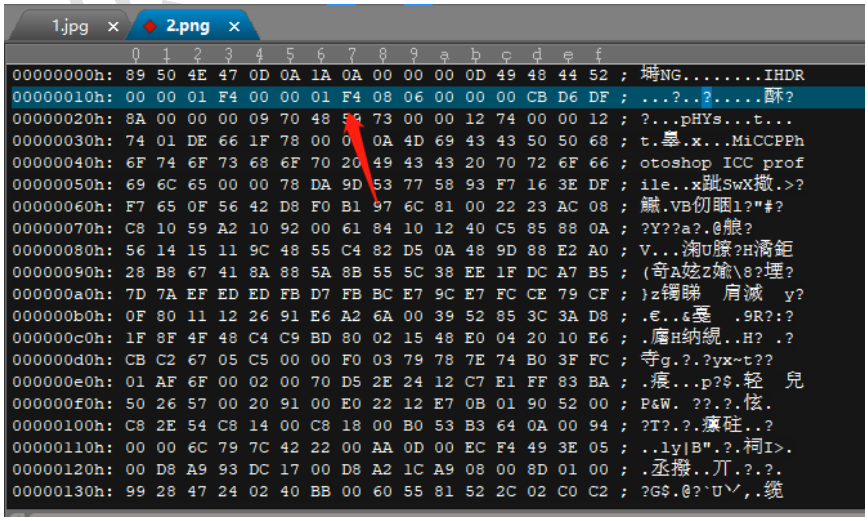
文件头数据块由13字节组成，它的格式如下表所示。

域的名称	字节数	说明
Width	4 bytes	图像宽度，以像素为单位
Height	4 bytes	图像高度，以像素为单位

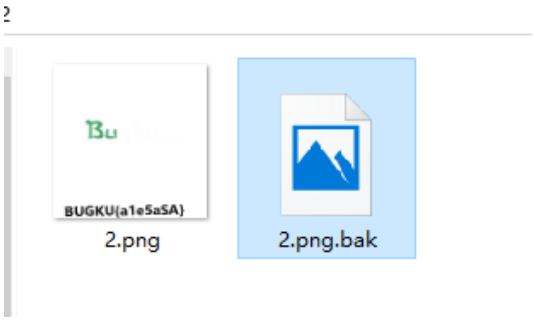
在 UE 中找到 **IHDR，在这之后的八个 bit 就是宽高的值**



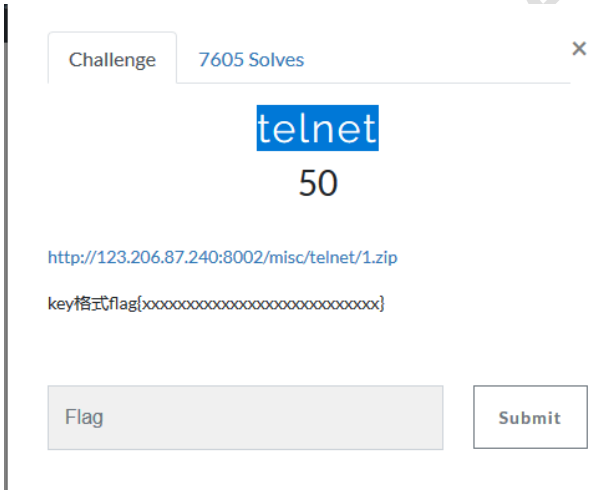
最后试出来是把高改成和宽一样即把 A4 改成 F4



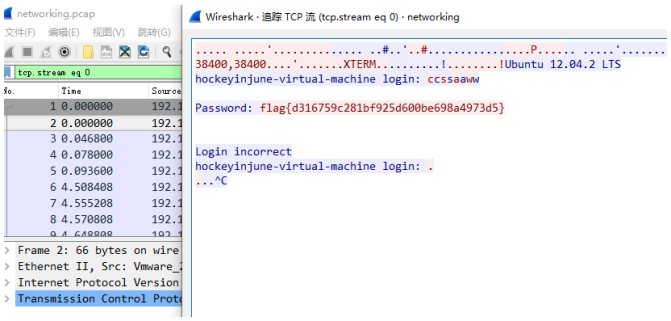
然后保存回到目录去看，flag 到手



杂项第四题: telnet

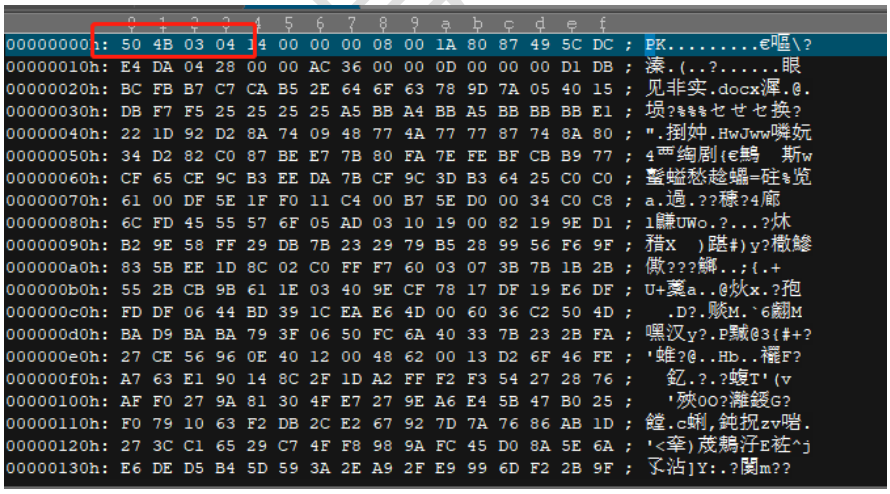


访问路径下载一个 1.zip
解压得到一个
用 wireshark 打开
任意一处右键追踪流，TCP 流，即可发现 flag

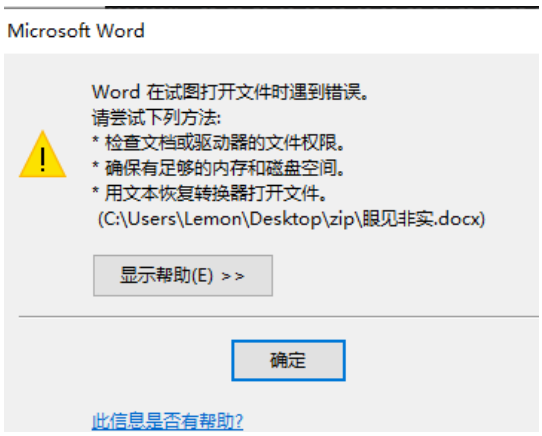


杂项第五题：眼见非实(ISCCCTF)

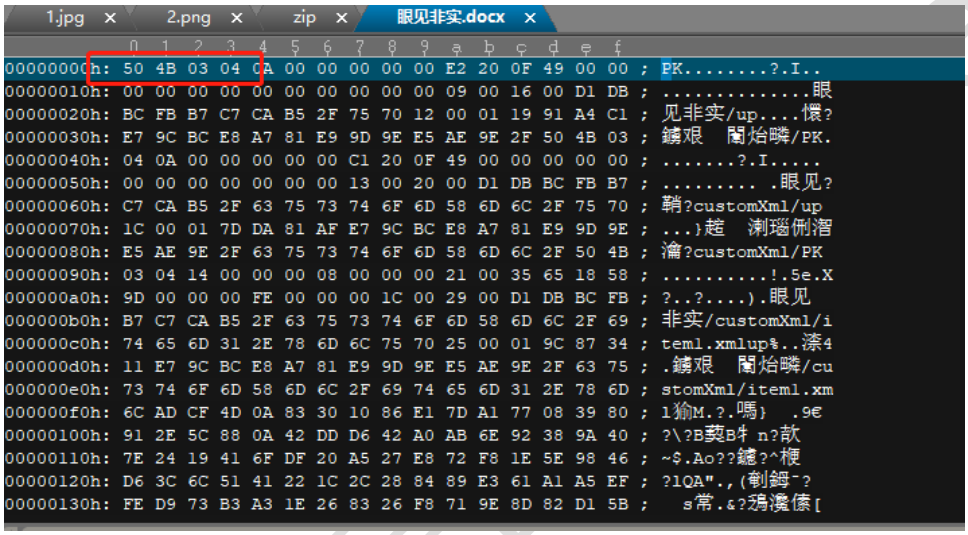
https://ctf.bugku.com/files/919ee4ea1658c3e3ef8b59b67f298470/zip
下载文件后，用 UE 打开

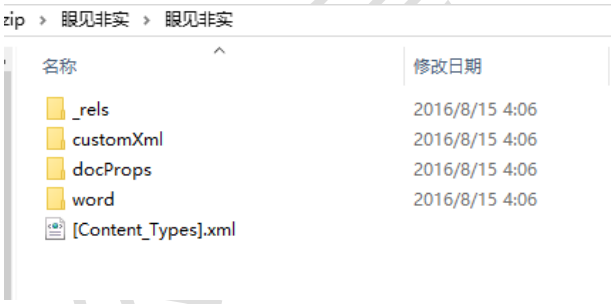


发现文件头为 50 4B 03 04 说明是一个压缩文件，还可以看到其中有.docx 文件
更改文件后缀为 .zip 解压后发现



这个文件用 word 是打不开的。。。 用 UE 打开发现这个还是个压缩文件，再次改后缀解压





眼见非实\word\document.xml 打开发现 flag

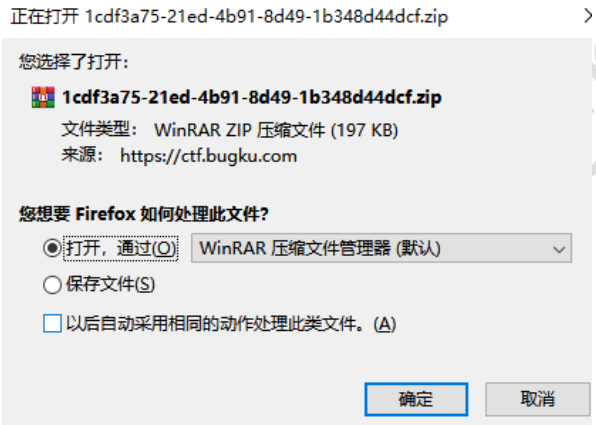
关于压缩文件头

Offset	Bytes	Description	译
0	4	Local file header signature = 0x04034b50 (read as a little-endian number)	文件头标识，值固定(0x04034b50)
4	2	Version needed to extract (minimum)	解压文件所需 pkware最低版本
6	2	General purpose bit flag	通用比特标志位(置比特0位=加密，详情见后)
8	2	Compression method	压缩方式（详情见后）
10	2	File last modification time	文件最后修改时间
12	2	File last modification date	文件最后修改日期
14	2	CRC-32	CRC-32校验码
18	4	Compressed size	压缩后的大小
22	4	Uncompressed size	未压缩的大小
26	2	File name length (n)	文件名长度
28	2	Extra field length (m)	扩展区长度
30	n	File name	文件名
30+n	m	Extra field	扩展区

杂项第六题:啊哒

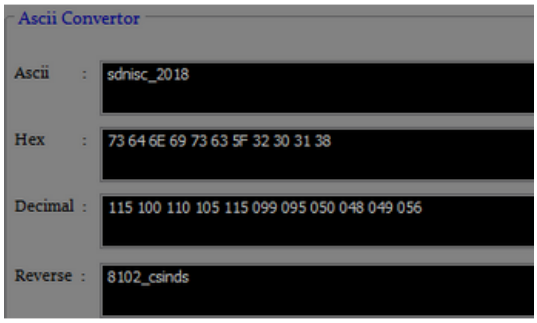
https://ctf.bugku.com/files/37b57dc545752a92fa6b2d571b88667a/1cdf3a75-21ed-4b91-8d49-1b348d44dcf.zip

下载压缩包



解压后得到一个图片

先看下图片属性，发现点东西，73646E6973635F32303138 将 16 进制转换成 ASCII 码的到 sdnisc_2018



在 linux 环境下用 binwalk 打开，发现里面有 zip 文件，利用 dd 命令分割一下

dd if=ada.jpg of=adazip skip=218773 bs=1

```
root@kali:/mnt/hgfs/ctf# binwalk ada.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image d
5236          0x1474          Copyright string: "Copyright Apple Inc., 2018"
218773        0x35695         Zip archive data, encrypted at least v2.0 to extract
218935        0x35737         End of Zip archive, footer length: 22

root@kali:/mnt/hgfs/ctf# dd if=ada.jpg of=adazip skip=218773 bs=1
记录了184+0 的读入
记录了184+0 的写出
```

将得到的 zip 解压，发现需要密码，把刚才的到的字符串 sdnisc_2018 输入，得到 flag.txt

```
root@kali:/mnt/hgfs/ctf# unzip adazip
Archive:  adazip
[adazip] flag.txt password:
 extracting: flag.txt
```

flag{3XiF_iNf0rM@ti0n}

这个题的考点就是，对于文件属性的查看，binwalk 工具与 dd 的使用

关于 dd 命令

dd [option]

dd 指令选项详解

if=file：输入文件名，缺省为标准输入
of=file：输出文件名，缺省为标准输出
ibs=bytes：一次读入 bytes 个字节（即一个块大小为 bytes 个字节）
obs=bytes：一次写 bytes 个字节（即一个块大小为 bytes 个字节）
bs=bytes：同时设置读写块的大小为 bytes ，可代替 ibs 和 obs

cbs=bytes：一次转换 bytes 个字节，即转换缓冲区大小
skip=blocks：从输入文件开头跳过 blocks 个块后再开始复制
seek=blocks：从输出文件开头跳过 blocks 个块后再开始复制。（通常只有当输出文件是磁盘或磁带时才有效）
count=blocks：仅拷贝 blocks 个块，块大小等于 ibs 指定的字节数
conv=ASCII：把 EBCDIC 码转换为 ASCII 码。
conv=ebcdic：把 ASCII 码转换为 EBCDIC 码。
conv=ibm：把 ASCII 码转换为 alternate EBCDIC 码。
conv=block：把变动位转换成固定字符。
conv=ublock：把固定位转换成变动位。
conv=ucase：把字母由小写转换为大写。
conv=lcase：把字母由大写转换为小写。
conv=notrunc：不截短输出文件。
conv=swab：交换每一对输入字节。
conv=noerror：出错时不停止处理。
conv=sync：把每个输入记录的大小都调到 ibs 的大小（用 NUL 填充）。

iflag=FLAGS：指定读的方式 FLAGS，参见“FLAGS 参数说明”
oflag=FLAGS：指定写的方式 FLAGS，参见“FLAGS 参数说明”
FLAGS 参数说明：
append -append mode (makes sense only for output; conv=notrunc sug-gested)
direct：读写数据采用直接 IO 方式；
directory：读写失败除非是 directory；
dsync：读写数据采用同步 IO；
sync：同上，但是针对是元数据
fullblock：堆积满 block（accumulate full blocks of input ）(iflag only)；
nonblock：读写数据采用非阻塞 IO 方式
noatime：读写数据不更新访问时间

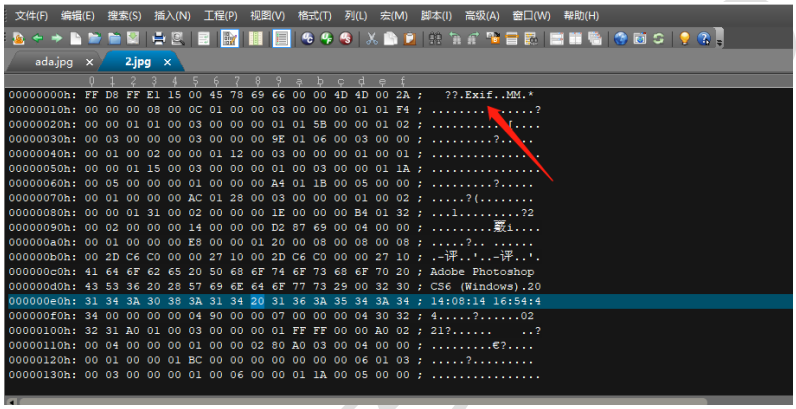
杂项第七题：又一张图片，还单纯吗

打开图片，保存到本地

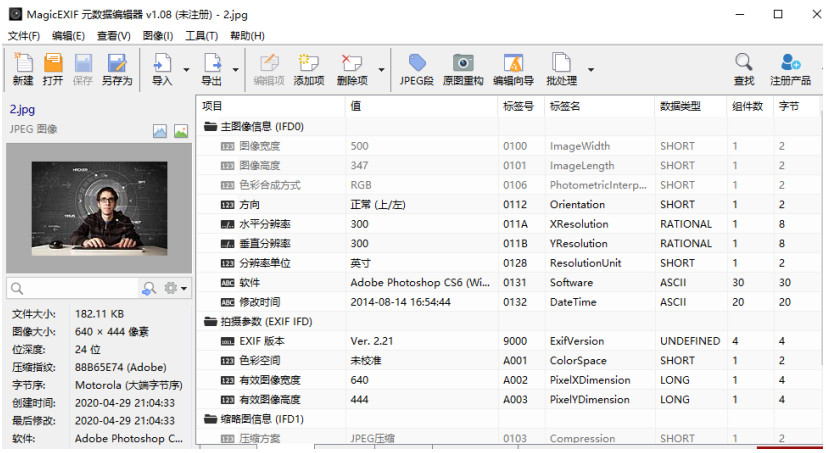
还是先看下图片属性

没什么发现

用 UE 随便看了下文件头和文件尾，没有发现字符串，但是看到文件头有 EXIF 信息。



于是找出 MagicExif 工具查看一下这个图片的 Exif 信息



结果是没有发现。

于是拿出 binwalk 查看有没有其他文件隐藏在图片中

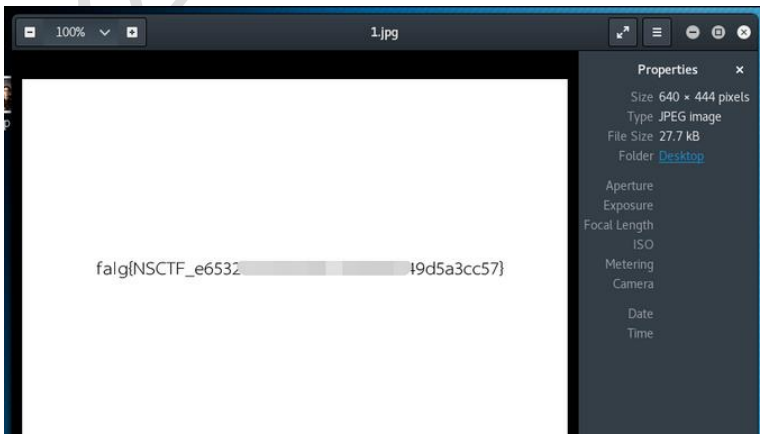
```
root@LAPTOP-OQE1H5K9:~/Desktop# binwalk -e 2.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, EXIF standard
12            0xC             TIFF image data, big-endian, offset of first imag
 directory: 8
13017         0x32D9          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#":
 <rdf:Description rdf:about="" xmlns:photoshop="http://ns.adobe.com/photoshop/1
0/" xmlns
158792        0x26C48         JPEG image data, JFIF standard 1.02
158822        0x26C66         TIFF image data, big-endian, offset of first imag
 directory: 8
159124        0x26D94         JPEG image data, JFIF standard 1.02
162196        0x27994         JPEG image data, JFIF standard 1.02
164186        0x2815A         Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#":
 <rdf:Description rdf:about="" xmlns:dc="http://purl.org/dc/elements/1.1/" xmln
:xap="htt
168370        0x291B2         Copyright string: "Copyright (c) 1998 Hewlett-Pac
ard Company"
```

发现捆绑了好几个图片文件。

用 dd 命令提取其中一个图片文件看下。
dd if=2 of=1.jpg skip=158792 bs=1

```
root@LAPTOP-OQE1H5K9:~/Desktop# dd if=2.jpg of=1.jpg skip=158792 bs=1
27689+0 records in
27689+0 records out
27689 bytes (28 kB, 27 KiB) copied, 0.0677667 s, 409 kB/s
```

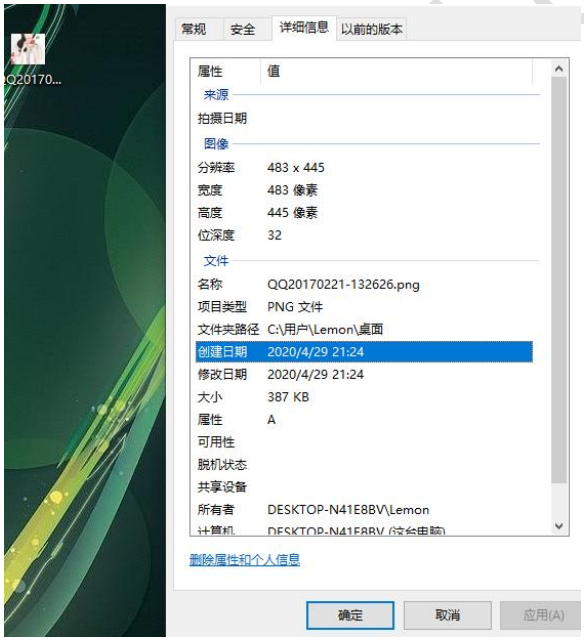
查看提取出来的图片文件，flag 到手。



falg{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

杂项第八题：猜

http://123.206.87.240:8002/misc/cai/QQ20170221-132626.png
打开图片保存到本地
查看属性无发现



其实是我想复杂了，题目标题是猜..推测应该不是考察的隐写术
要猜图片人的名字，但图片只给了半张脸，想到百度识图。

图片来源

范爷同款白成一道光~

网上购物介绍网 >>对于范爷同款白成一道光~网上购物折扣价格与评价 网上购物介绍网 >>对于范爷同款白成一道光~网上购物折扣价格...

ok.pai-hang-bang.cn

还在化妆p图?她只是把直发换成了卷发

▲只卷一边啊姑娘们,无论如何都要把一半肩膀露出来!而且下巴以上绝对保持直发,防止脑袋显得过大!

ent.k618.cn

春季刊封面女星斗艳连连看_第一女人网

刘亦菲　　再来看看《时尚芭莎》4月下封面大片，刘亦菲化身古典美人，早已在网上掀起一轮热赞。 人面桃花相映红，此次妆容再适...

fashion.miss-no1.com

女星代表性的唇形,终于知道什么唇形好看了-不得不八卦

power-bd.com

我们都是认识，是刘亦菲

Flag 到手 key{liuyifei}