
杂项题目练习（一）

杂项题目练习	1
杂项第一题: 签到题.....	4
杂项第二题: 这是一张单纯的图片	5
杂项第三题: 隐写	7
杂项第四题: telnet	9
杂项第五题: 眼见非实(ISCCCTF).....	10
杂项第六题: 啊哒.....	13
杂项第七题: 又一张图片, 还单纯吗	15
杂项第八题: 猜.....	18

前言：

以下是在 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：

题目练习	1
杂项第一题: 签到题	3
杂项第二题: 这是一张单纯的图片	4
杂项第三题: 隐写	6
杂项第四题: telnet	8
杂项第五题: 眼见非实(ISCCCTF)	9
杂项第六题: 啊哒	12
杂项第七题: 又一张图片, 还单纯吗	14
杂项第八题: 猜	17
杂项第九题: 宽带信息泄露	19
杂项第十题: 隐写 2	20
杂项第十一题: 多种方法解决	23
杂项第十二题: 闪的好快	25
杂项第十三题: come_game	26
杂项第十四题: 白哥的鸽子	28
杂项第十五题: linux	30
杂项第十六题: 隐写 3	30
杂项第十七题: 做个游戏(08067CTF)	33
杂项第十八题: 想蹭网先解开密码	35
杂项第十九题: Linux2	39
杂项第二十题: 细心的大象	42
杂项第二十一题: 爆照(08067CTF)	47
杂项第二十二题: 猫片(安恒)	51
杂项第二十三题: 旋转跳跃	57
音频工具 MP3stego 使用 (一)	59
音频工具 MP3stego 使用 (二)	60
杂项第二十四题: 普通的二维码	61
CTF 杂项之音频及视频隐写补充	64
杂项第二十五题: 乌云邀请码	71
杂项第二十六题: CTF 之隐写术--LSB 一张图片隐藏的信息	73
杂项第二十七题: convert	76
杂项第二十八题: 听首音乐	80
杂项第二十九题: ctf 练习---摩斯密码	83
杂项第三十题: 好多数值	84
杂项第三十一题: 神秘的文件	87
杂项第三十二题: 三十 zip 明文攻击	90
杂项第三十三题: 论剑	91

杂项第三十四题: 图穷匕见.....	94 ^u
杂项第三十五题: 很普通的数独(ISCCTF)	99 ^u
杂项第三十六题: PEN_AND_APPLE	103 ^u
NTFS 数据流及高级文件隐藏.....	105 ^u
杂项第三十七题: color	107 ^u
杂项第三十八题: 小明的密码.....	110 ^u
杂项第三十九题: 仿射加密.....	111 ^u
仿射密码解析与实例.....	113 ^u
杂项第四十题: 黑客的机密信息	117 ^u
杂项第四十一题: 远控木马.....	118 ^u
杂项第四十二题: Web 漏洞	118 ^u
bugku-ctf 第四十三题: 颜文字	120 ^u
杂项第四十四题: 磁盘镜像.....	120 ^u
杂项第四十五题: 神奇的图片	121 ^u
杂项第四十六题: 怀疑人生	122 ^u
杂项第四十七-CTF 加密篇之 ok (Ook!)	129 ^u
杂项第四十八题: 红绿灯.....	131 ^u
杂项第四十九题: 不简单的压缩包.....	136 ^u

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

Challenge 10438 Solves x

签到题
50

关注微信公众号: Bugku
即可获取flag

下面也有二维码

qrcode_for_gh_d...

Flag

Submit



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

Challenge 10439 Solves X

这是一张单纯的图片

50

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

FLAG在哪里? ?

Flag Submit

打开后

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

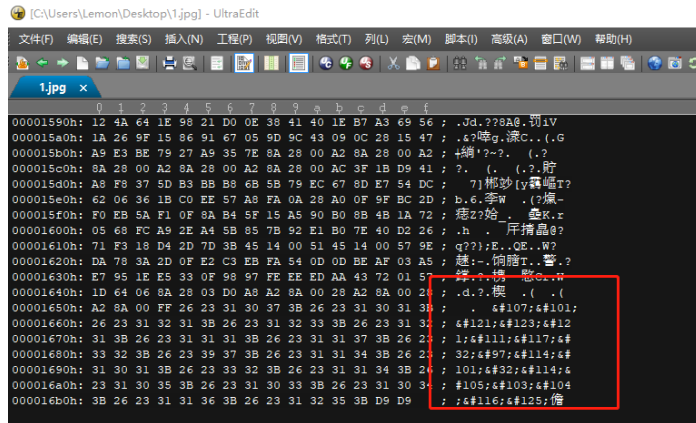


打开题目所给的链接, 发现是一张图片, 应该是考察隐写术。右击保存图片到本地。



先看了一眼文件属性, 没有什么发现。。

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



key{you are rig
ht}

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



key{you are right}

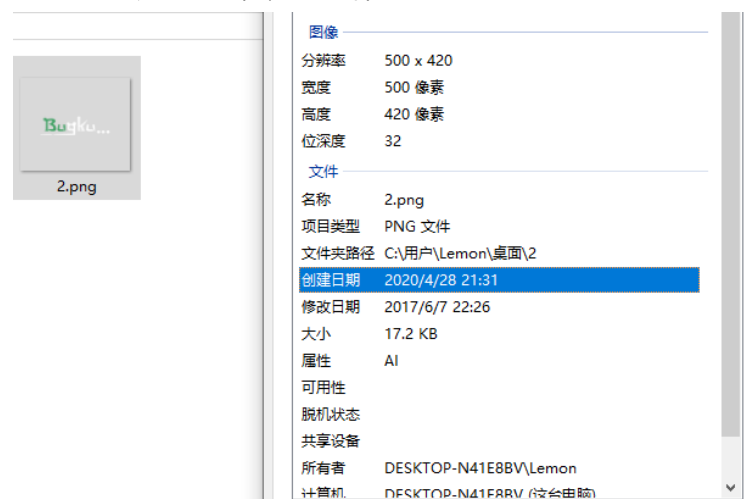
杂项第三题: 隐写



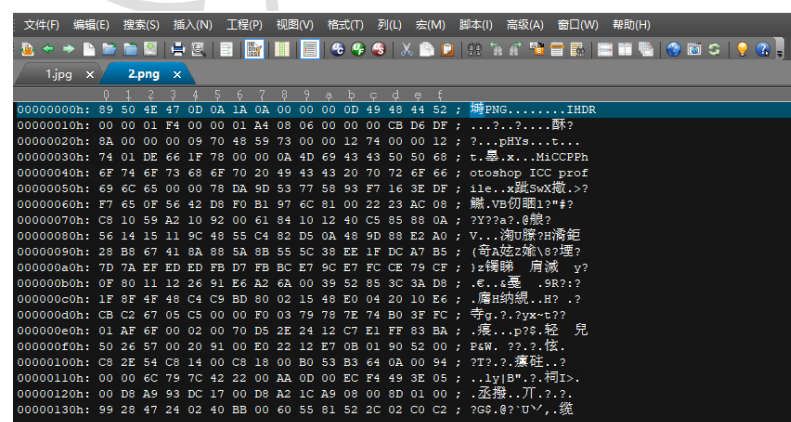
下载压缩包

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

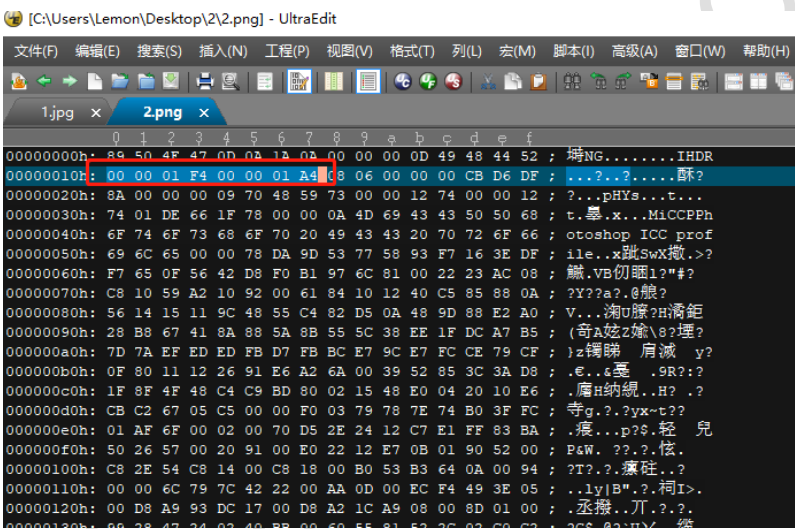
IHDR

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。

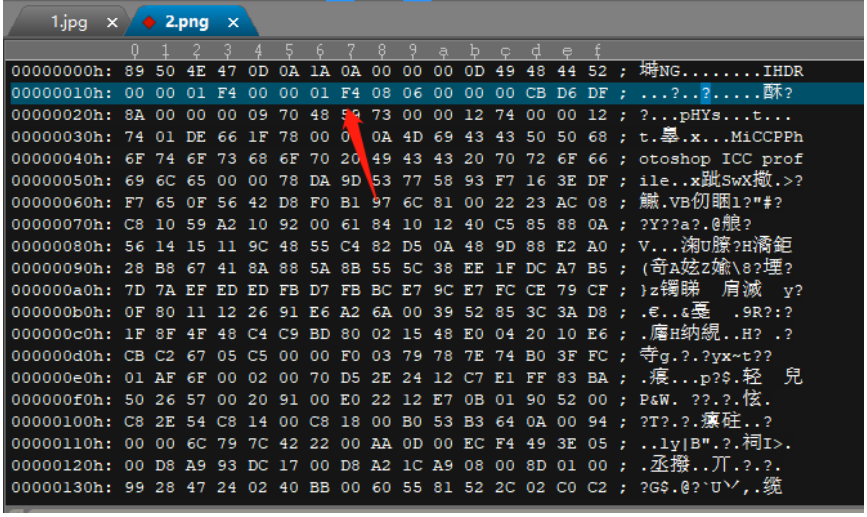
文件头数据块由13字节组成，它的格式如下表所示。

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

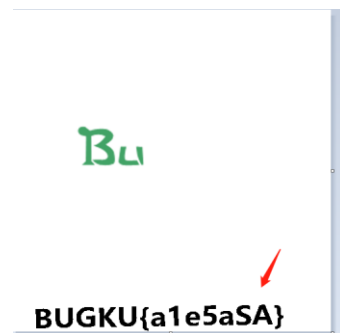
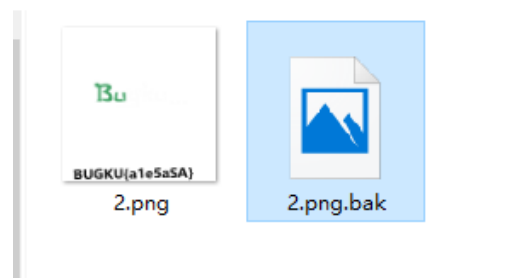


最后试出来是把高改成和宽一样即把 A4 改成 F4



然后保存回到目录去看，flag 到手

2



杂项第四题: telnet

Challenge 7605 Solves ×

telnet
50

<http://123.206.87.240:8002/misc/telnet/1.zip>

key格式flag{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}

Flag

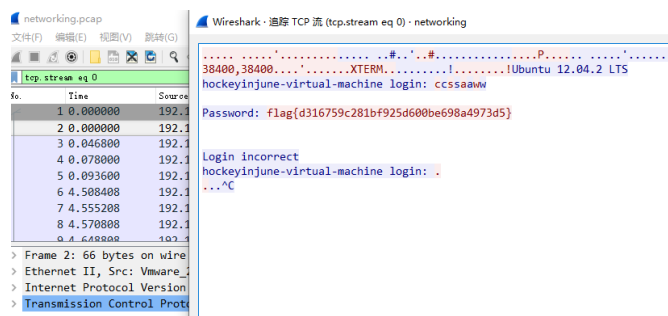
Submit

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)

Challenge 6886 Solved

眼见非实(ISCCCTF)

50

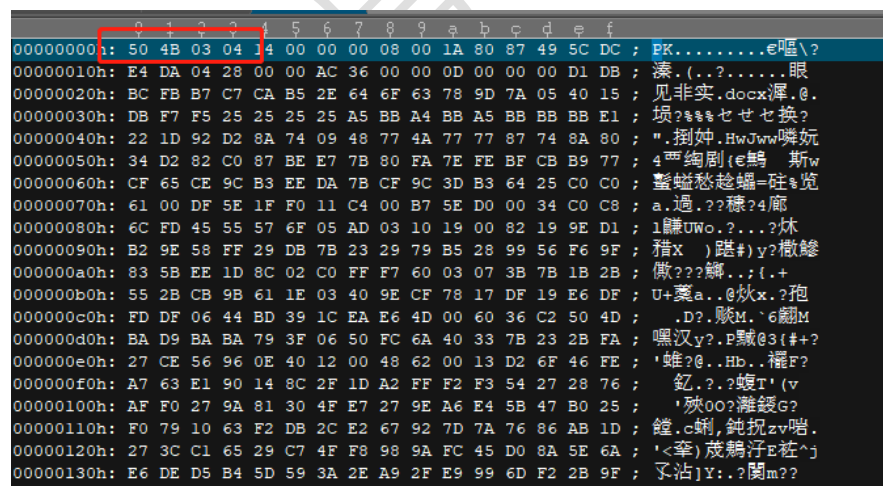
zip

Flag

Submit

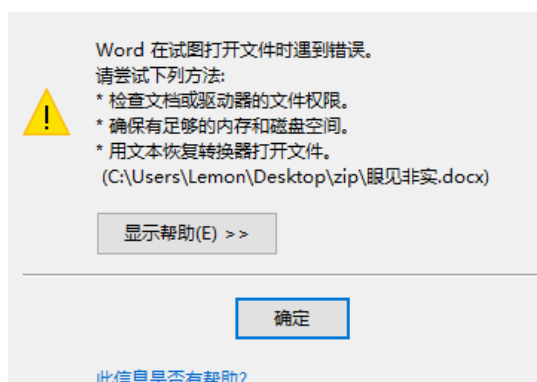
<https://ctf.bugku.com/files/919ee4ea1658c3e3ef8b59b67f298470/zip>

下载文件后, 用 UE 打开

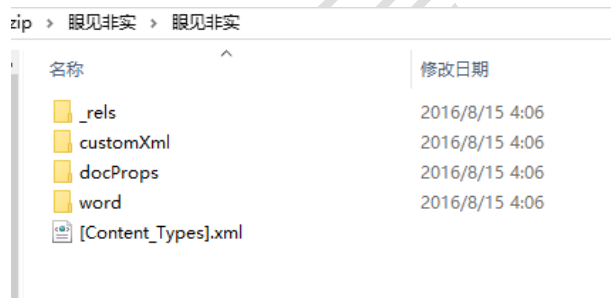
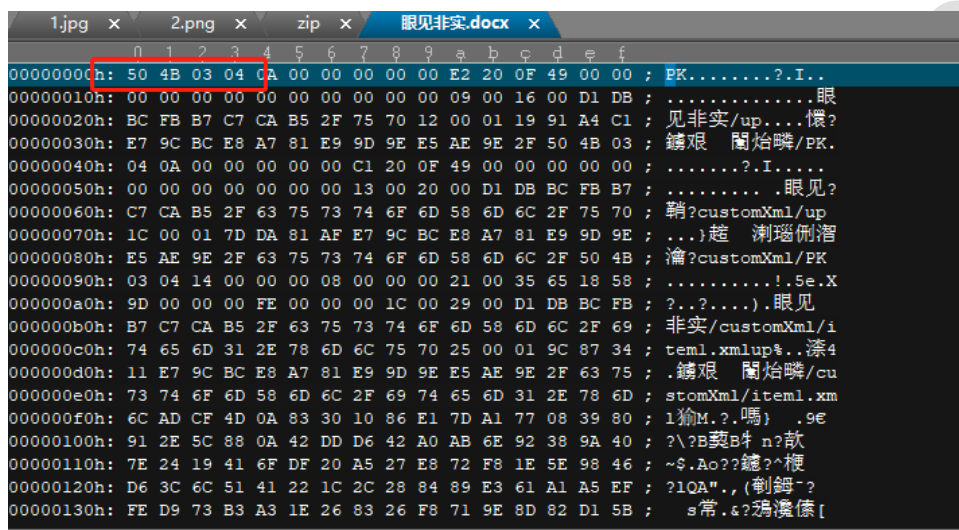


发现文件头为 50 4B 03 04 说明是一个压缩文件, 还可以看到其中有.docx 文件
更改文件后缀为 .zip 解压后发现

Microsoft Word



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

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<w:document xmlns:wp="http://schemas.microsoft.com/office/word/2010/wordprocessingCanvas"
  xmlns:mc="http://schemas.openxmlformats.org/markup-compatibility/2006" xmlns:o=
"urn:schemas-microsoft-com:office:office" xmlns:r="
http://schemas.openxmlformats.org/officeDocument/2006/relationships" xmlns:m="
http://schemas.openxmlformats.org/officeDocument/2006/math" xmlns:v=
"urn:schemas-microsoft-com:vml" xmlns:wp14="
http://schemas.microsoft.com/office/word/2010/wordprocessingDrawing" xmlns:wp="
http://schemas.openxmlformats.org/drawingml/2006/wordprocessingDrawing" xmlns:w10=
"urn:schemas-microsoft-com:office:word" xmlns:w="
http://schemas.openxmlformats.org/wordprocessingml/2006/main" xmlns:w14="
http://schemas.microsoft.com/office/word/2010/wordml" xmlns:w15="
http://schemas.microsoft.com/office/word/2012/wordml" xmlns:wpg="
http://schemas.microsoft.com/office/word/2010/wordprocessingGroup" xmlns:wpi="
http://schemas.microsoft.com/office/word/2010/wordprocessingInk" xmlns:wne="
http://schemas.microsoft.com/office/word/2006/wordml" xmlns:wps="
http://schemas.microsoft.com/office/word/2010/wordprocessingShape" mc:Ignorable="w14 w15
wp14"><w:body><w:p w:rsidR="002B3D8D" w:rsidRDefault="002B3D8D"><w:r><w:t>Flag
</w:t></w:r><w:r><w:t>在这里哟! </w:t></w:r></w:p><w:p w:rsidR="002B3D8D" w:rsidRPr=
"002B3D8D" w:rsidRDefault="002B3D8D"><w:pPr><w:rPr><w:font w:hint="eastAsia"/><w:vanish
/></w:rPr></w:pPr><w:r w:rsidRPr="002B3D8D"><w:rPr><w:vanish/></w:rPr><w:t>flag(F1@g)
</w:t></w:r><w:bookmarkStart w:id="0" w:name="GoBack"/><w:bookmarkEnd w:id="0"/>
</w:p><w:sectPr w:rsidR="002B3D8D" w:rsidRPr="002B3D8D"><w:pgSz w:w="11906" w:h="16838"/>
<w:pgMar w:top="1440" w:right="1800" w:bottom="1440" w:left="1800" w:header="851"
w:footer="992" w:gutter="0"/><w:cols w:space="425"/><w:docGrid w:type="lines" w:linePitch
="312"/></w:sectPr></w:body></w:document>
```

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

Challenge 4397 Solves X

啊哒

50

有趣的表情包
来源：第七届山东省大学生网络安全技能大赛

1cdf3a75-21ed-...

Flag

Submit

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

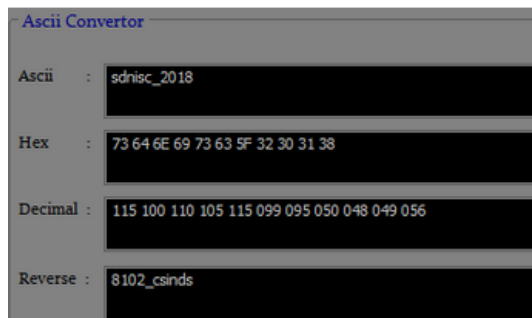
下载压缩包



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

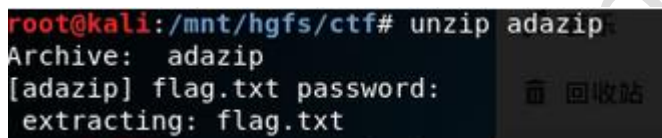




在 linux 环境下用 binwalk 打开，发现里面有 zip 文件，利用 dd 命令分割一下
dd if=ada.jpg of=adazip skip=218773 bs=1



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



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=lc case: 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 suggested)
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

Challenge

5070 Solves

×

又一张图片, 还单纯吗

60

<http://123.206.87.240:8002/misc/2.jpg>

好像和上一个有点不一样

Flag

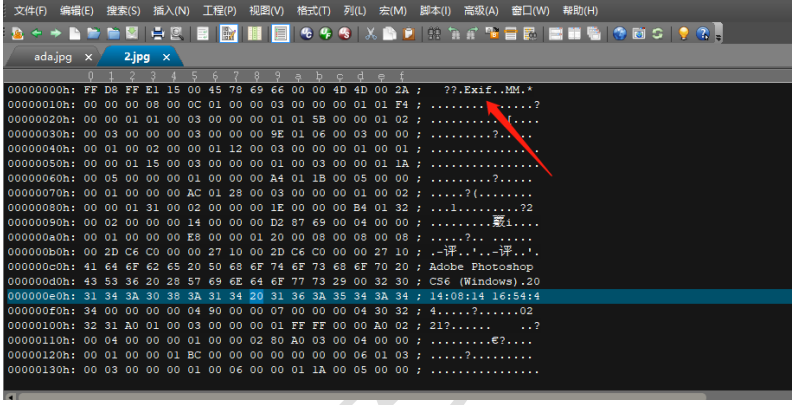
Submit

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。



Exif

编辑

讨论

上传视频

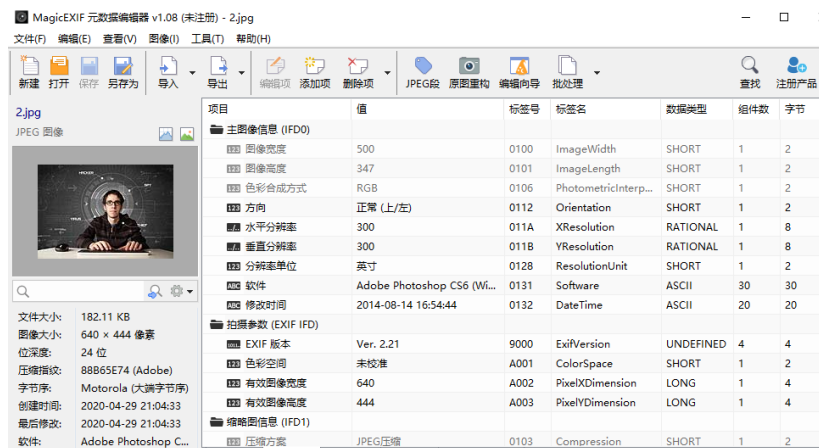
本词条由 科普中国 科学百科词条编写与应用工作项目 审核。

可交换图像文件格式（英语：Exchangeable image file format，官方简称**Exif**），是专门为**数码相机**的照片设定的，可以记录数码照片的属性信息和拍摄数据。

Exif最初由日本电子工业发展协会在1996年制定，版本为1.0。1998年，升级到2.1，增加了对音频文件的支持。2002年3月，发表了2.2版。

中文名	Exif	支持类型	JPEG、TIFF、RAW等
外文名	Exchangeable Image File	释 义	可交换图像文件格式
类 型	图像文件格式	作 用	记录数码照片的属性信息和拍摄数据

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 image 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:dc="http://purl.org/dc/elements/1.1/" xmlns:xap="http://www.adobe.com/xap/1.0/"
158792	0x26C48	JPEG image data, JFIF standard 1.02
158822	0x26C66	TIFF image data, big-endian, offset of first image 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/" xmlns:xap="http://www.adobe.com/xap/1.0/"
168370	0x291B2	Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"

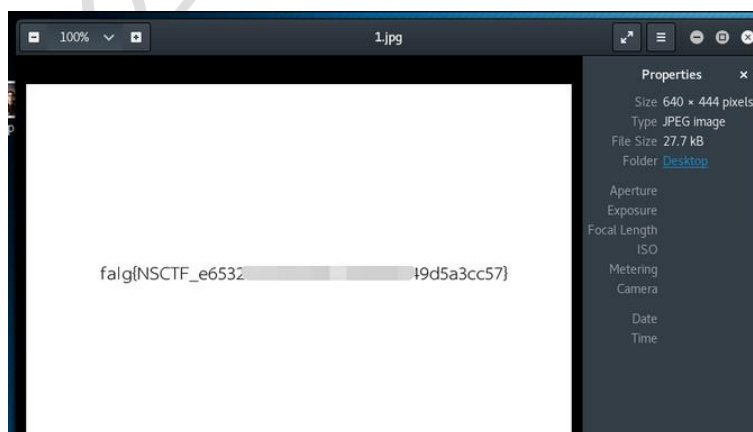
发现捆绑了好几个图片文件。

用 dd 命令提取其中一个图片文件看下。

dd if=2.jpg 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。



flag{NSCTF_e6532a34928a3d1dadd0b049d5a3cc57}

杂项第八题: 猜

Challenge 6195 Solves X

猜
60

<http://123.206.87.240:8002/misc/cai/QQ20170221-132626.png>

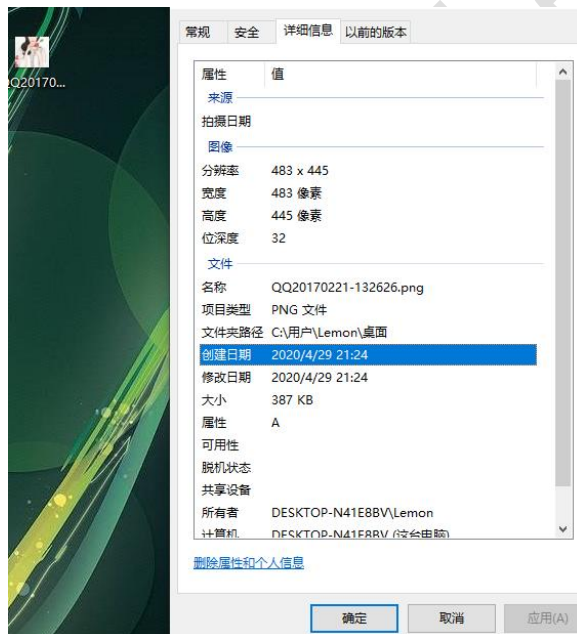
flag格式key{某人名字全拼}

Flag Submit

<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,此次妆容再道...
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}