BugKu ——WP（MISC[一]）

原创

窝窝头_233 于 2019-11-26 10:58:43 发布 157 收藏

分类专栏： CTFwriteup 文章标签： ctf BugKuCTF

本文链接：https://blog.csdn.net/hahaha233330/article/details/103252311

BugKu —— MISC部分

- [0]工具

①Winhex：图片隐写工具，可通过搜索“ctf”“CTF”“key”“flag”等关键字得到flag。
②在线工具HtmlEncode/BASE64转换：注意源代码里奇怪的字符串，可以尝试解码（分清类型）。
③Binwalk：可查看多重文件。使用说明
④VMware（kali_Linux）：虚拟机，方便解压。

MISC

- **1、签到题**
  关注微信公众号：Bugku
  即可获取flag
  下面也有二维码

这题没什么好说的，扫码关注公众号即可得到flag。

- **2、这是一张单纯的图片**
  FLAG在哪里？？

把图片放到winhex，拉到最后一行可以看到如下奇怪的编码：

```
1D 64 06 8A 28 03 D0 A8  A2 8A 00 28 A2 8A 00 28   d Š( Ð¨¢Š (¢Š (
A2 8A 00 FF 26 23 31 30  37 3B 26 23 31 30 31 3B  ¢Š ÿ&#107;&#101;
26 23 31 32 31 3B 26 23  31 32 33 3B 26 23 31 32  &#121;&#123;&#12
31 3B 26 23 31 31 31 3B  26 23 31 31 37 3B 26 23  1;&#111;&#117;&#
33 32 3B 26 23 39 37 3B  26 23 31 31 34 3B 26 23  32;&#97;&#114;&#
31 30 31 3B 26 23 33 32  3B 26 23 31 31 34 3B 26  101;&#32;&#114;&
23 31 30 35 3B 26 23 31  30 33 3B 26 23 31 30 34  #105;&#103;&#104
3B 26 23 31 31 36 3B 26  23 31 32 35 3B D9 D9     ;&#116;&#125;ÙÙ
```

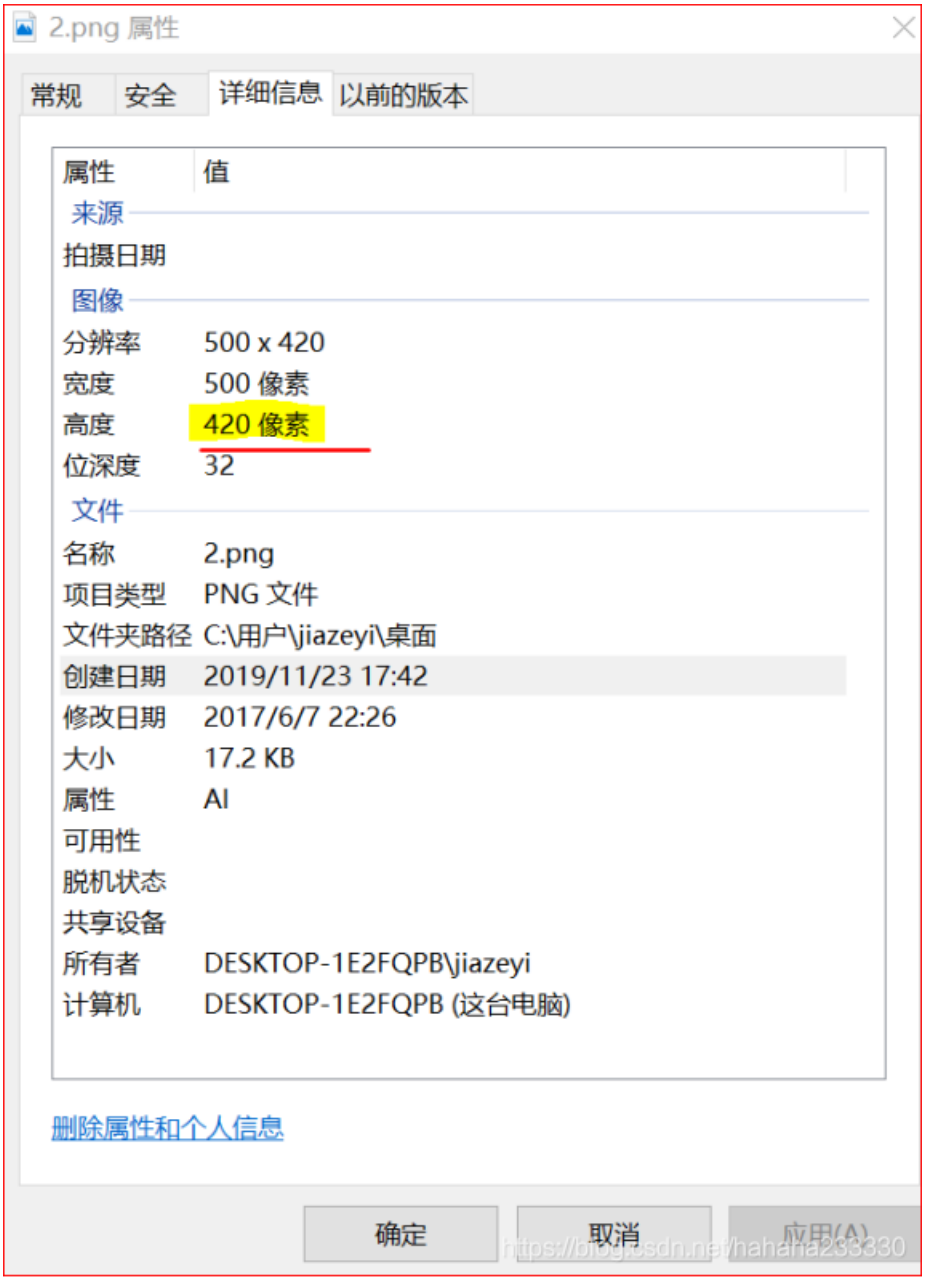

看类型是html编码，

通过在线解码器转换一下即可得到flag。

- **3、隐写**

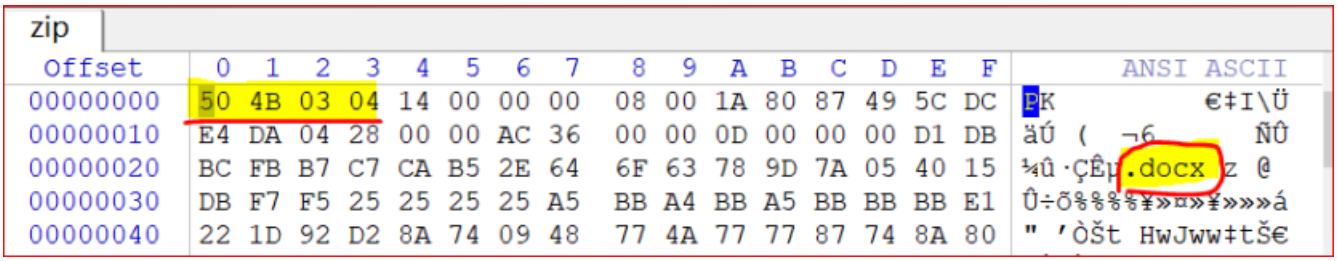
可以正常打开图片，鼠标右键查看一下图片的属性。

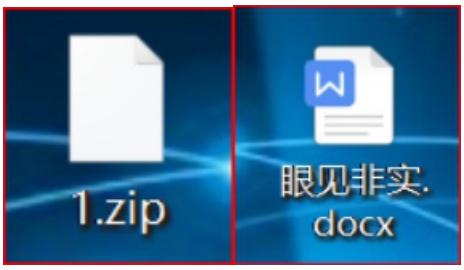
猜测可能是照片的宽和高信息被改了，放到 winhex 中尝试改宽高信息后发现是高被改了，将高修改为和宽一致即可得到flag。



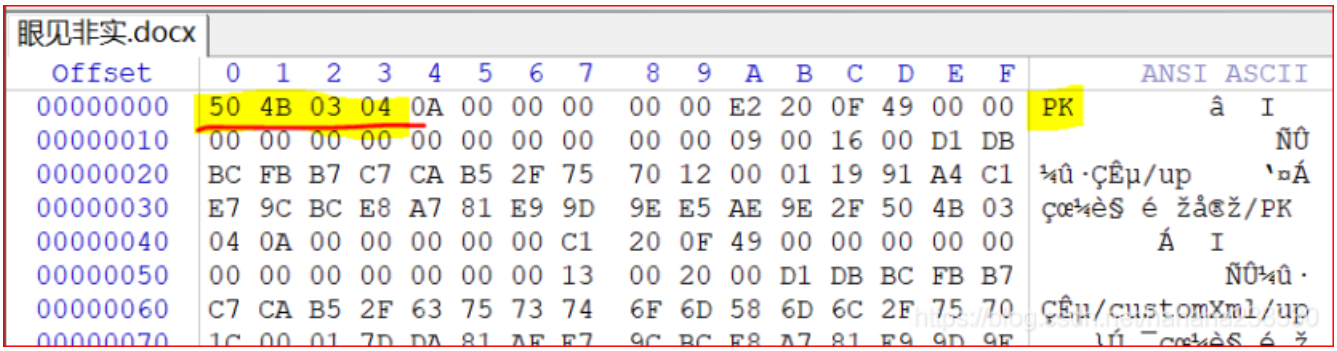
- **5、眼见非实（ISCCCTF）**

下载得到的是一个文件的格式，放到winhex中，发现有50 4B 03 04，这是压缩文件的头，而且发现还有 .docx 格式的文件，应该压缩包里有一个文档，改文件后缀为 .zip ，解压得到文档-眼见非实.docx。



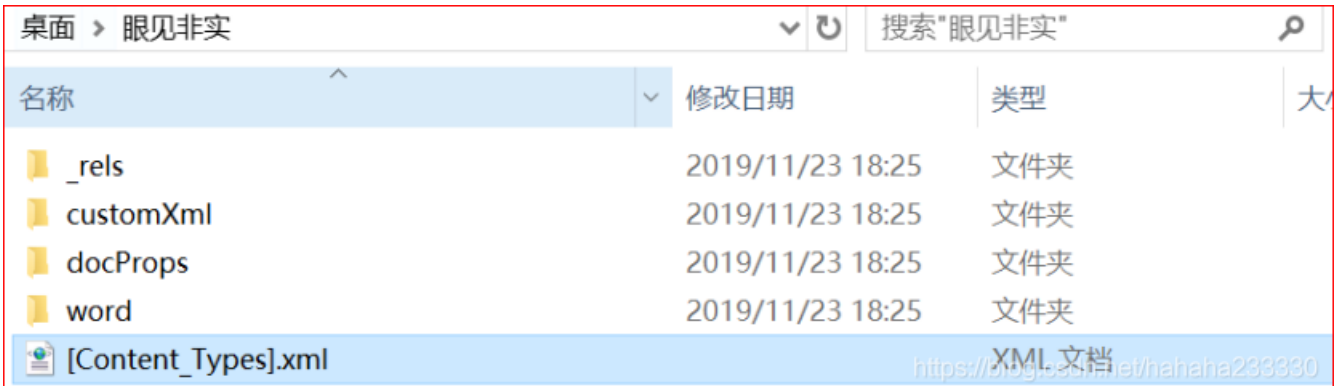


但是该文档打开后是乱码，再次放在winhex中查看，发现还是 .zip 的格式。



那就再次

改后缀为 .zip，再次解压，得到一个文件夹。



然后在

word->document.xml中找到了flag。

- **8、猜**

  题目地址

  flag格式key{某人名字全拼}

这题竟然真的盲猜，可以百度识图，我猜是***~

*注意flag格式：key{某人名字全拼}