CTF-安全杂项（十五）（涉及wireshark和winhex的使用）

原创

红烧兔纸 于 2019-01-15 21:04:01 发布 3122 收藏 12
分类专栏： CTF-安全杂项 文章标签： CTF

本文链接：https://blog.csdn.net/weixin_39934520/article/details/86498911

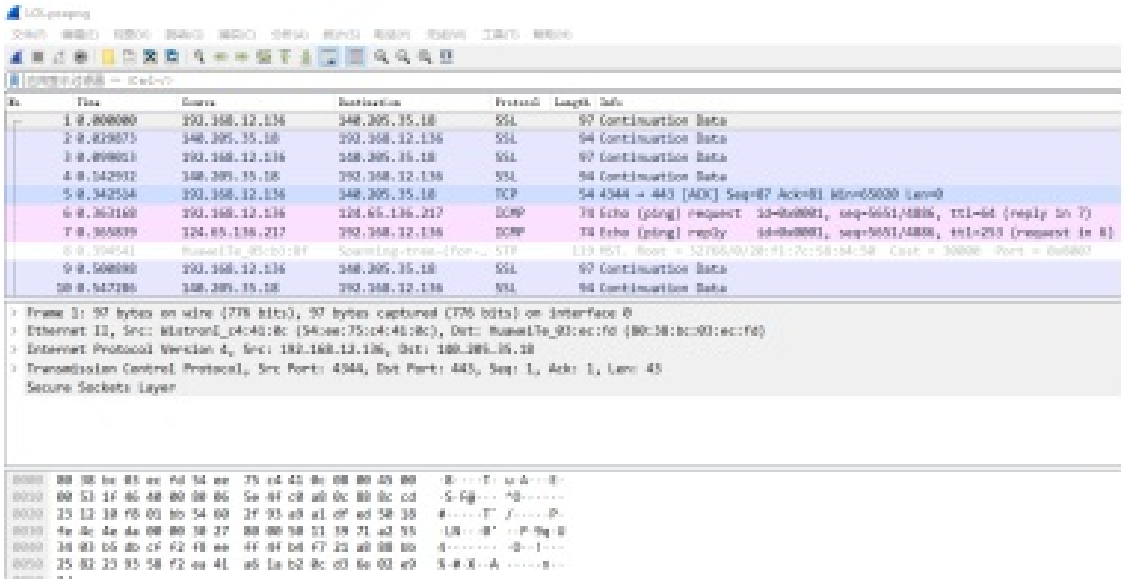
啦啦啦

分析：

（*+__+*）~ @ 受不了～ 这题对于wireshark都不会用的我来说，真是一点都不友好，摸索了半天，看了各路大神的WriteUp勉强拿到了flag。。。。

不说了，上图：

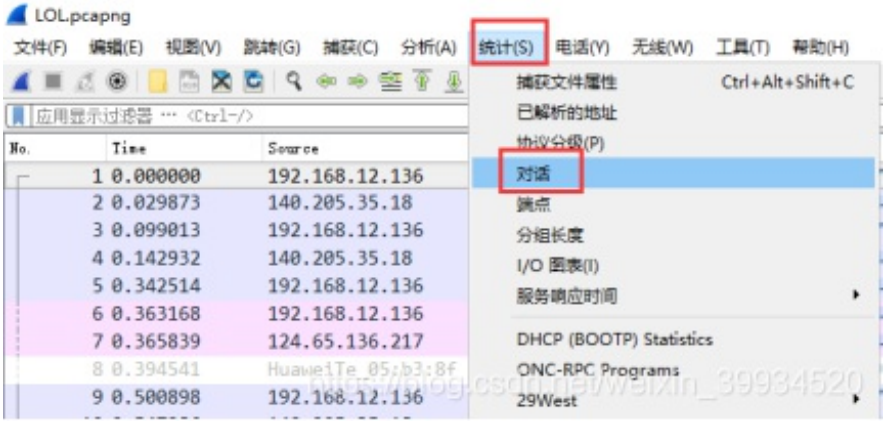
1.使用wireshark打开LOL.pcapng



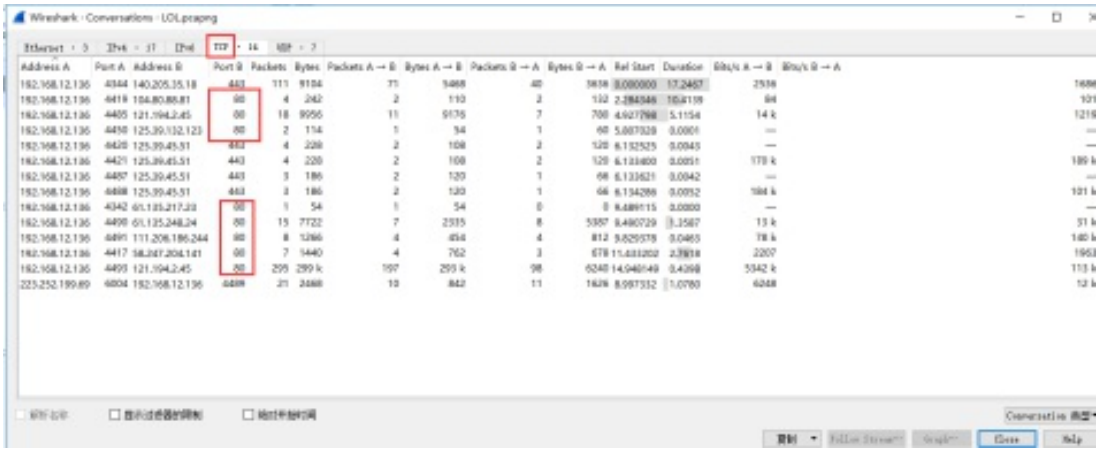
中文版wireshark----送给广大伸手党的同胞们：链接：https://pan.baidu.com/s/1Qq0i_BaCZHYar29PB8-mFw

提取码：op2x

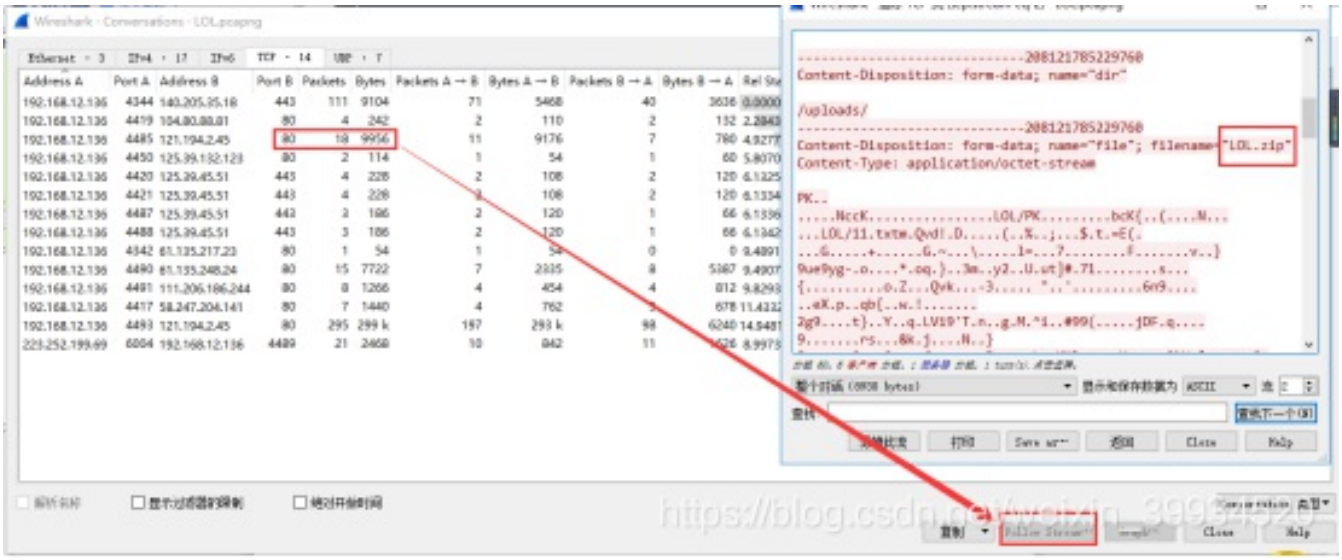
2.据说拿到数据包后，一般都是导出http对象。--发现了LOL.zip和lol.docx



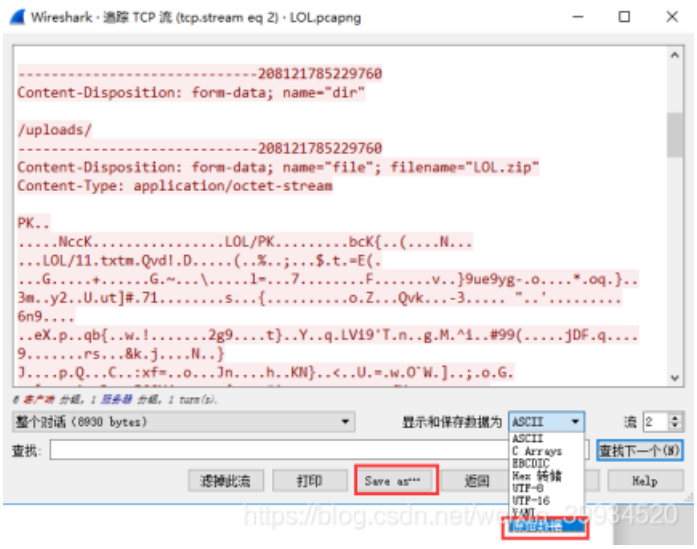
关注tcp协议的80端口

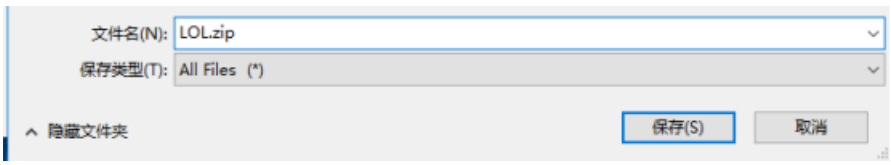


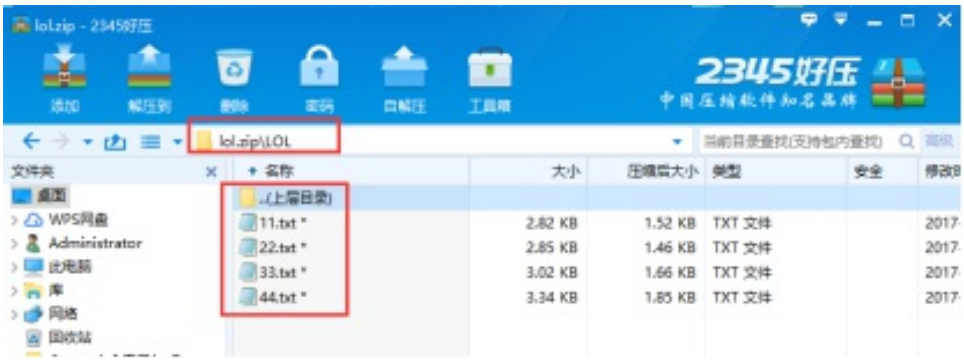
发现LOL.zip



导出LOL.zip：选择原始数据另存为LOL.zip

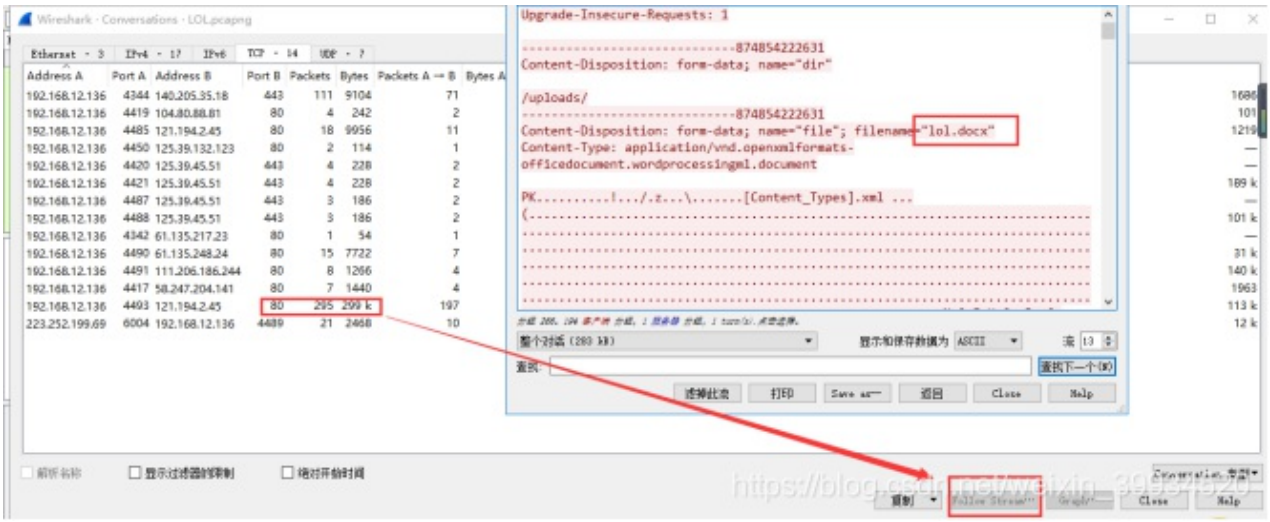






发现4个加密文档，先放一边。

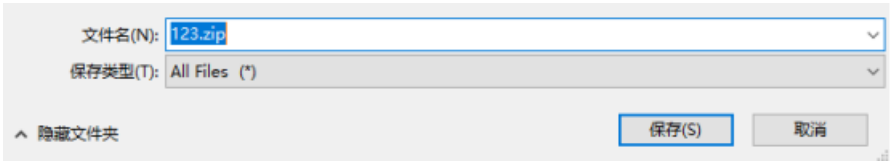
接下来继续导：



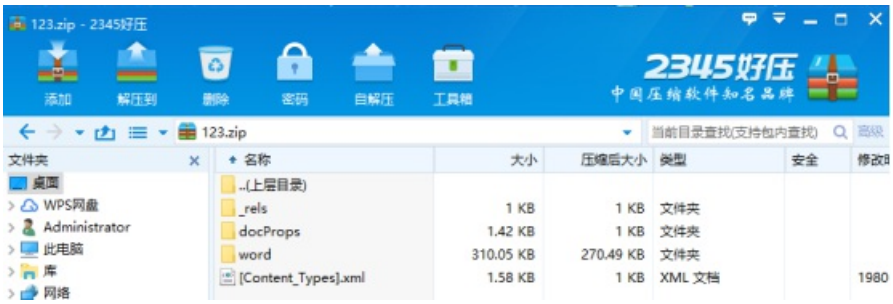
发现lol.docx

这里的docx本萌新实在是弄不出来， 

只能另辟蹊径，于是乎继续查资料，当看到这句“**word文档其本质就是一个压缩包。**”时，啊，我感觉我又有救了，果断保存为123.zip



查看，发现一大堆东西：



最有价值的信息就是一张图片：

这张图片无任何价值，因为docx版是这样的：

这几个字，我在压缩包里没找到，没办法，萌新就是这么菜。。。所以看你们的了，找到了，告诉我一下，让我也学着点。

##注：该问题我已解决，可以在本文章的最后看到。

1. 重点突破lol.zip

注：

一个 ZIP 文件由三个部分组成：

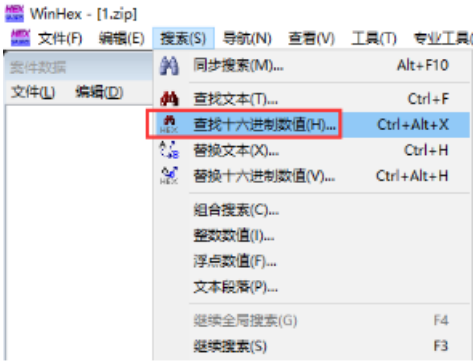
压缩源文件数据区+压缩源文件目录区+压缩源文件目录结束标志

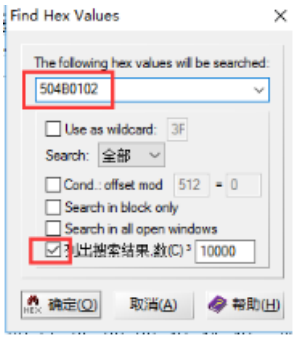
这里涉及zip的伪加密知识，不懂得，自行搜索资料，这里不再过多的赘述。。。

压缩源文件目录区：
50 4B 01 02：目录中文件文件头标记(0x02014b50)
3F 00：压缩使用的 pkware 版本
14 00：解压文件所需 pkware 版本
00 00：全局方式位标记（有无加密，偶加奇不加）

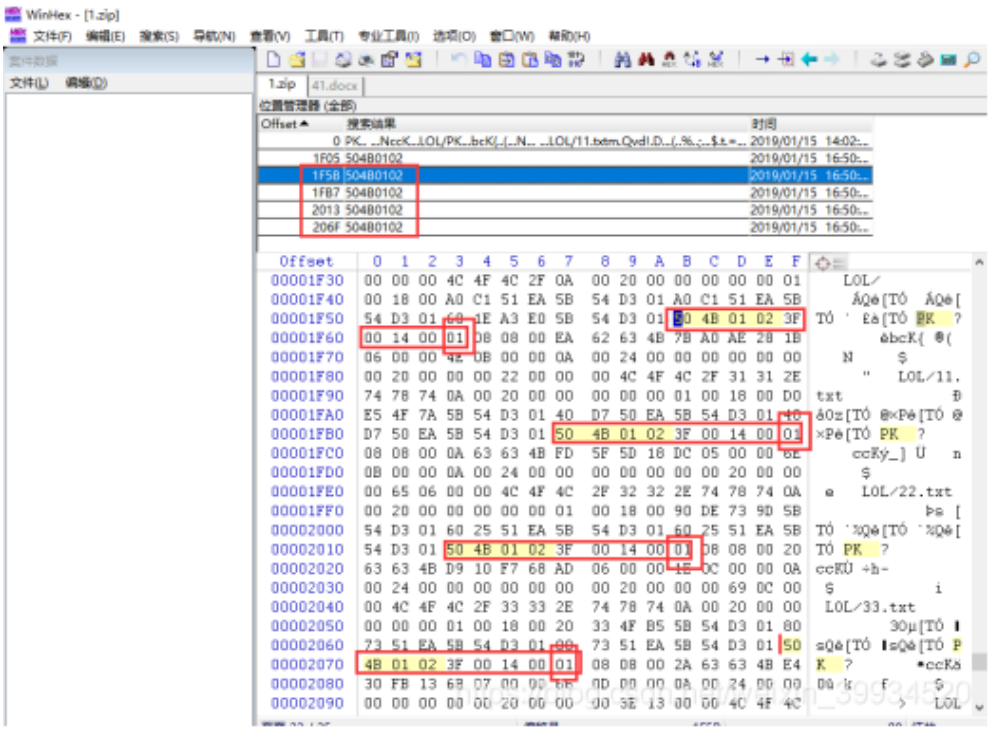
伪加密的特征，奇数结尾。

搜索压缩源文件目录区：

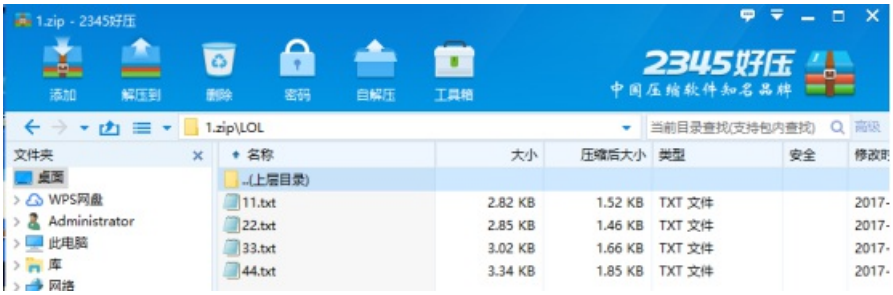




4个文档：

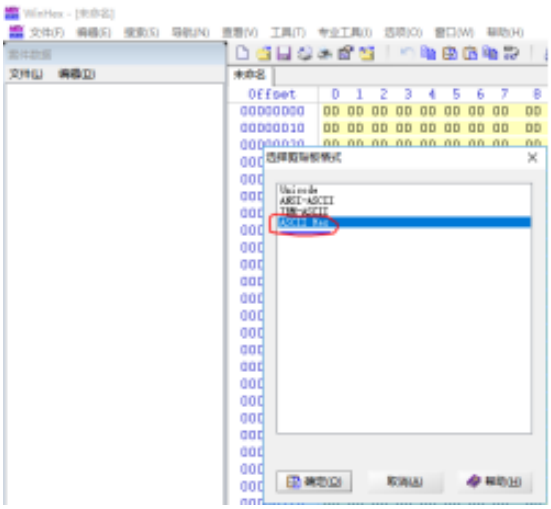


把奇数1可以改为偶数2，保存并打开：



文件解压后发现是4个16进制的文本，且都有89504E47，而png的文件头也是89504E47，猜测是4个png图片。

把他们复制到winhex中，注意选择ASCI HEX形式，然后保存：



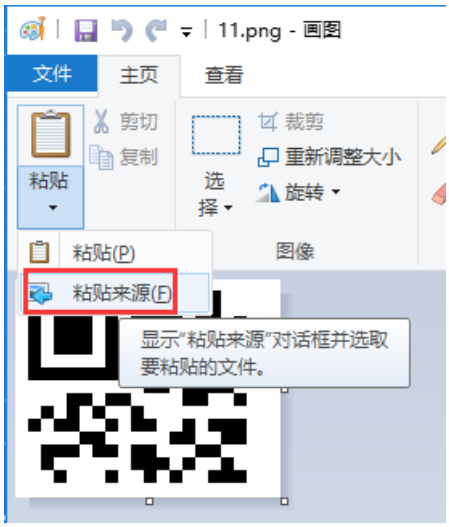
很明显这四个应该能和成一个正常的二维码：

听大神们说用PS合成一个二维码，本萌新不会PPPPPPPPPs啊，魂淡，继续查资料。。。

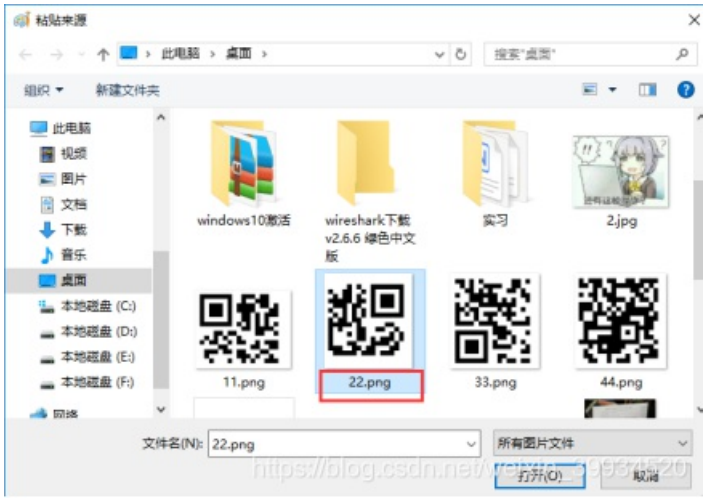
于是乎，画图神器出来了。。。。

来来画图工具走起：

先打开11.png再选择粘贴来源



然后选择另一张图片22.png



继续。。。

扫码：

http://jiema.wwei.cn/

或者用QR Research

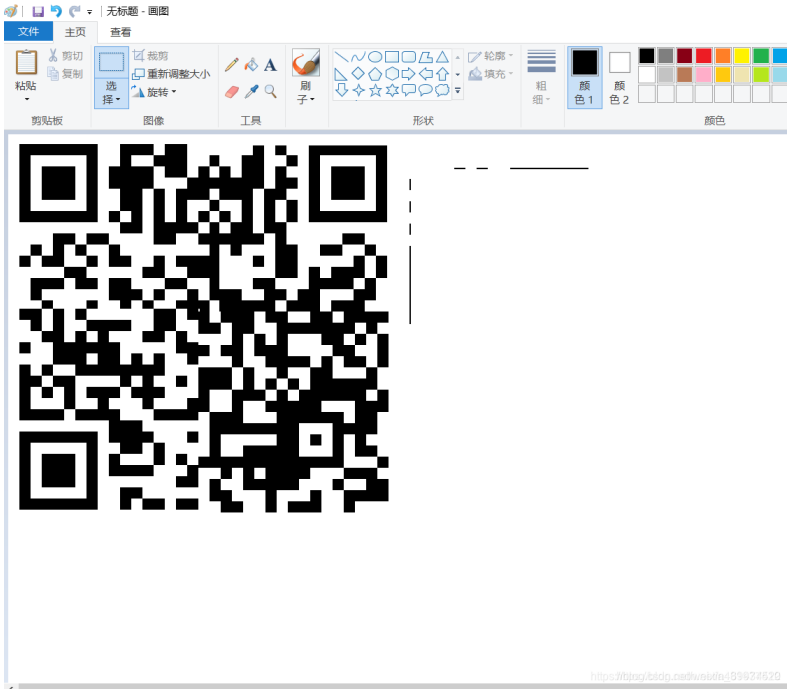
但是。。。。。

红色警告。。。红色警告。。。。

扫不出来。。。。。。。。有毒。。。

PS不会，剩下的看你们的了。。

这是我截取别人弄出来的图片扫描二维码即可得出答案：

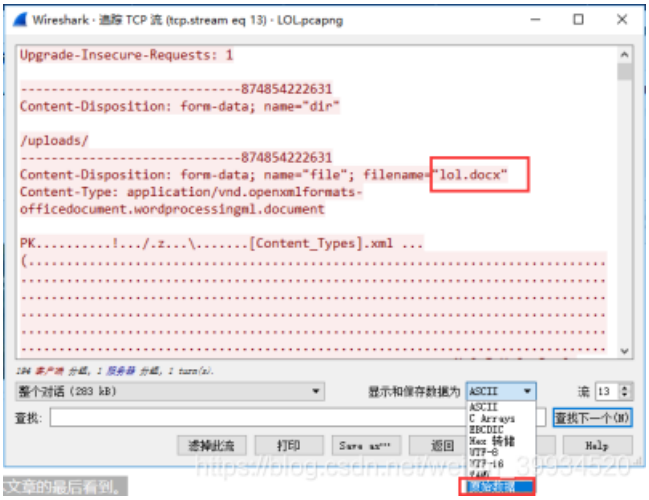


附上你们最喜欢的flag

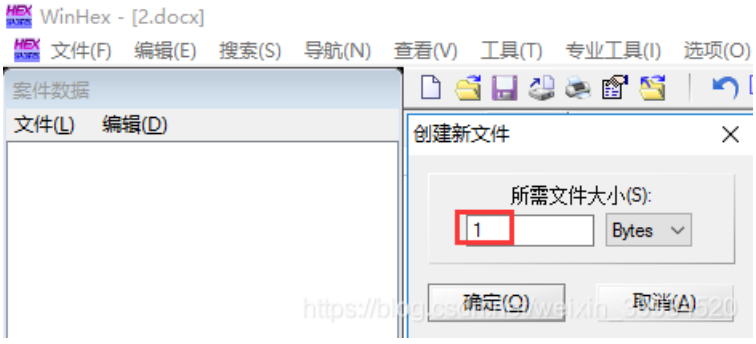
flag{NP3j4ZjF&syk9$5h@x9Pqac}

##获取文档：

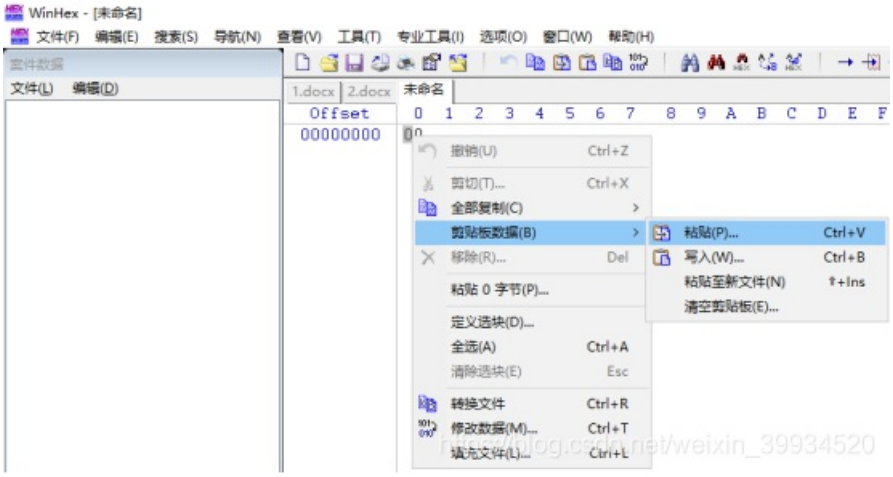
当发现文档时，我们以原始数据显示并全部复制



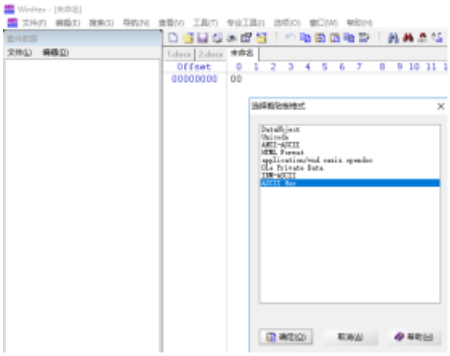
然后再在winhex中新建一个文件，大小随意，最好小一点，应为最后还是要删除的



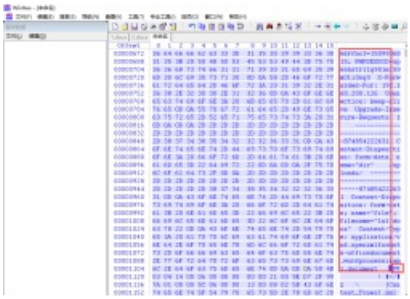
右键编辑--选择剪贴板数据-粘贴

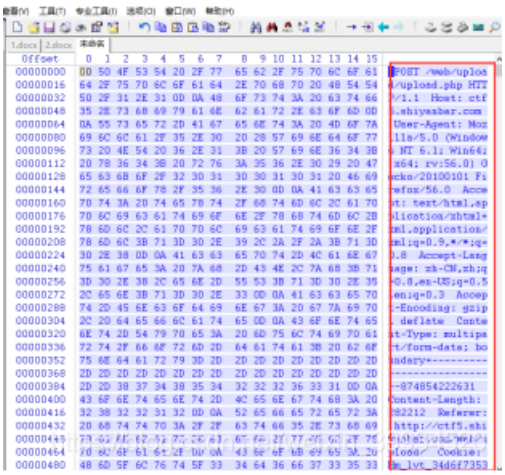


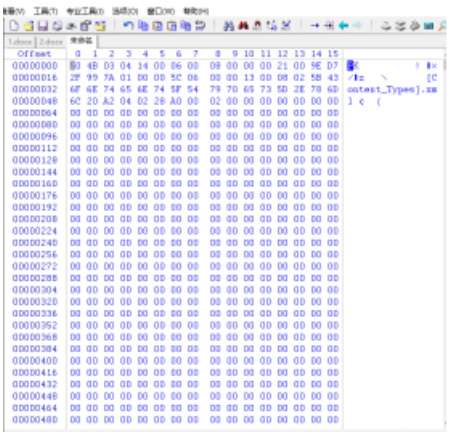
如果有其他弹窗直接确定，最重要的一点是要选择ASCII Hex 格式



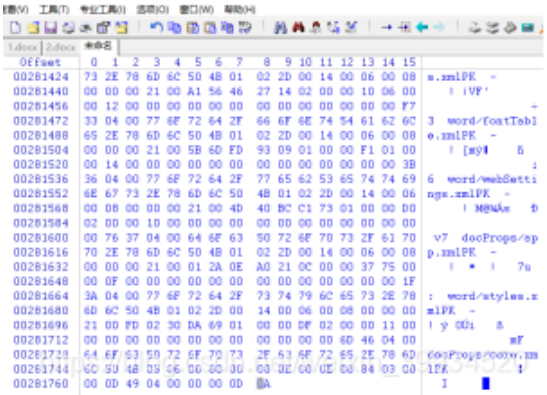
然后，把PK前的内容都删除：右键--编辑移除



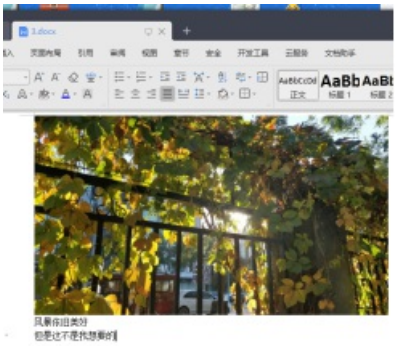




然后，把该文件的底部，PK I 后面的都删除



然后，保存为3.docx并打开：



补：其实删除的都是这些内容：