

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](#)

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/weixin_39934520/article/details/86498911

版权



[CTF-安全杂项](#) 专栏收录该内容

15 篇文章 1 订阅

订阅专栏

啦啦啦

啦啦啦 分值: 20

来源: 实验吧	难度: 易	参与人数: 3280人	Get Flag: 574人	答题人数: 832人	解题通过率: 69%
---------	-------	-------------	----------------	------------	------------

隐藏在数据包中的秘密

解题链接: <http://ctf5.shiyanbar.com/misc/LOL/LOL.pcapng> 通过

https://blog.csdn.net/weixin_39934520 提交

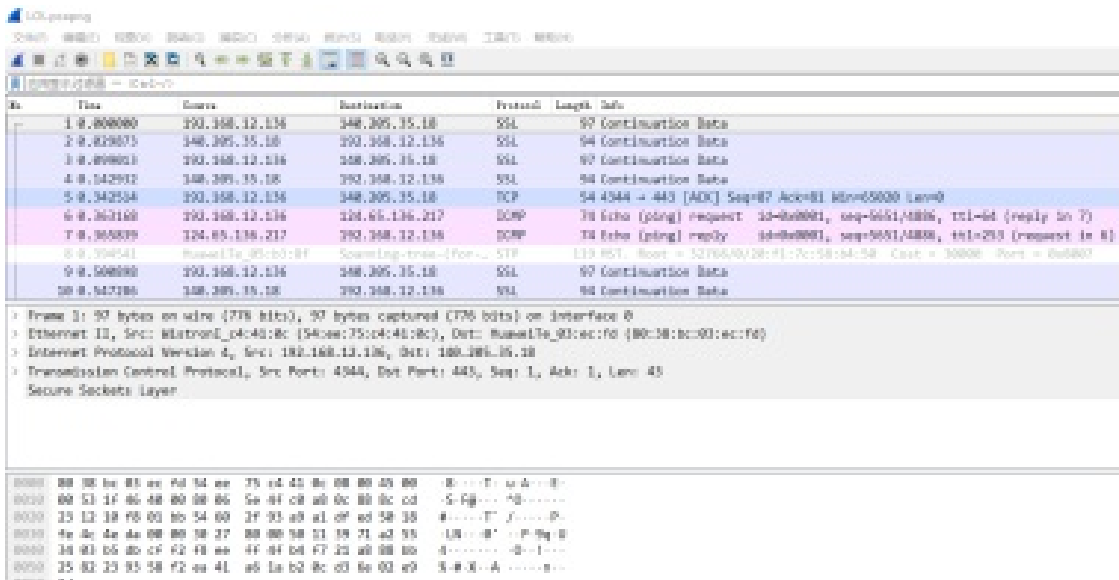
分析:

(*_+_*~) ~ @ 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。。。



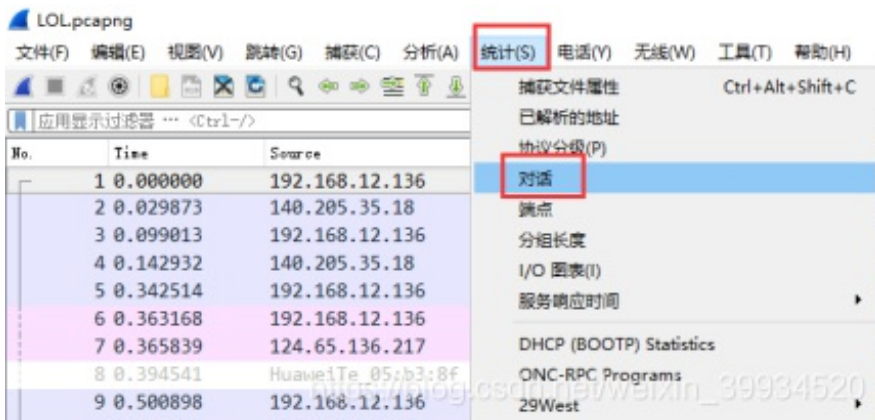
不说了, 上图:

1.使用wireshark打开LOL.pcapng

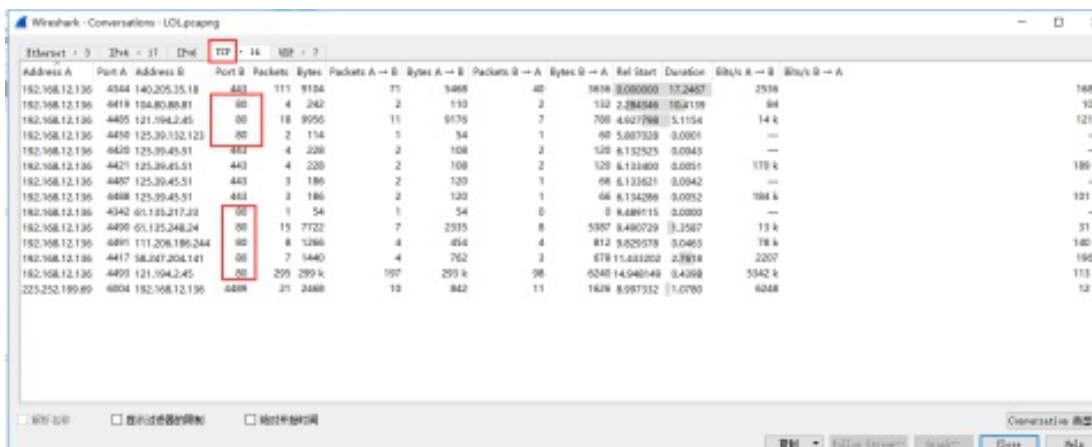


中文版wireshark----送给广大伸手党的同胞们：链接：https://pan.baidu.com/s/1Qq0i_BaCZHYar29PB8-mFw
提取码：op2x

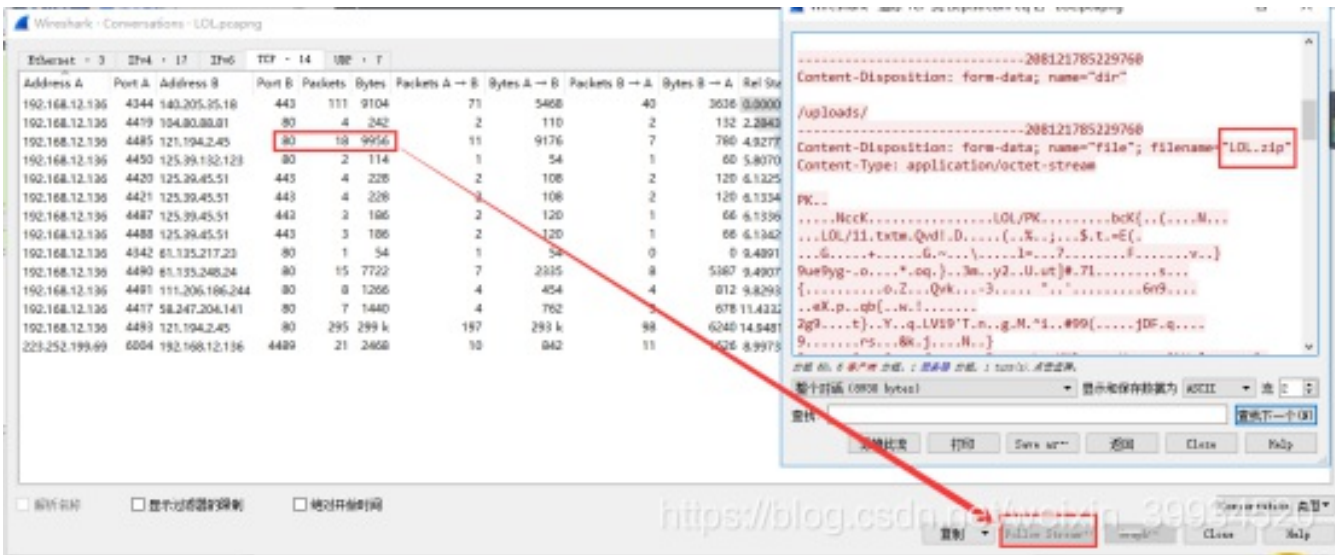
2.据说拿到数据包后，一般都是导出http对象。--发现了LOL.zip和lol.docx



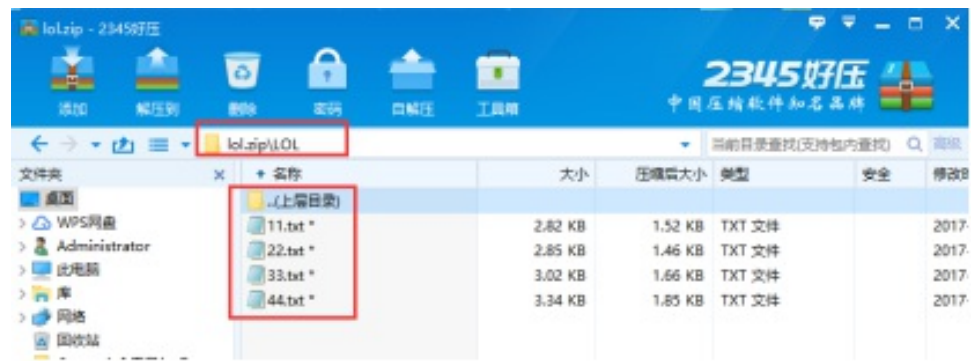
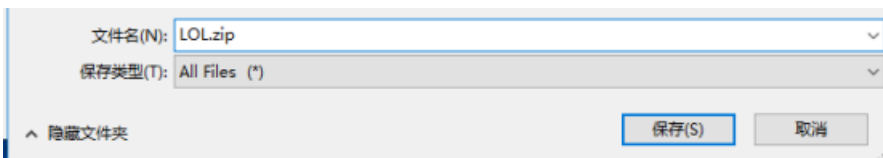
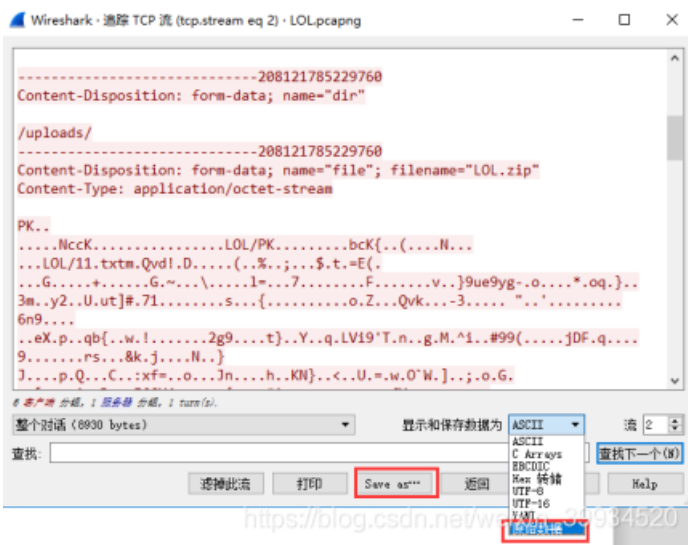
关注tcp协议的80端口



发现LOL.zip

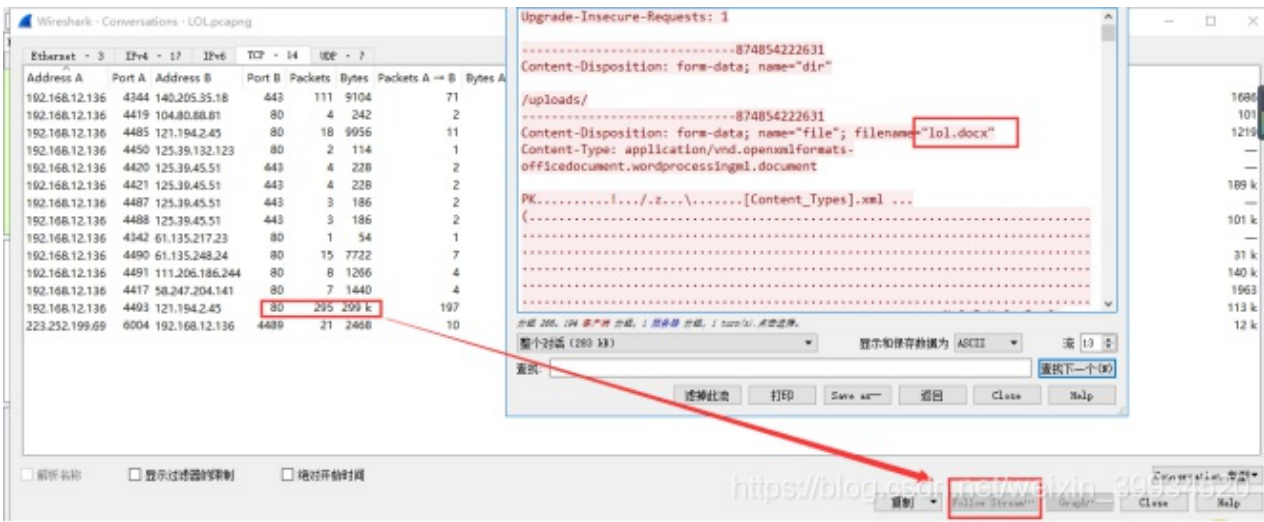


导出LOL.zip: 选择原始数据另存为LOL.zip



发现4个加密文档，先放一边。

接下来继续导：

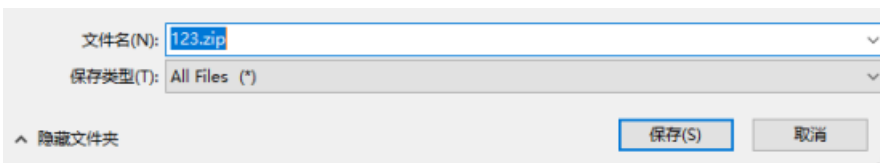


发现lol.docx

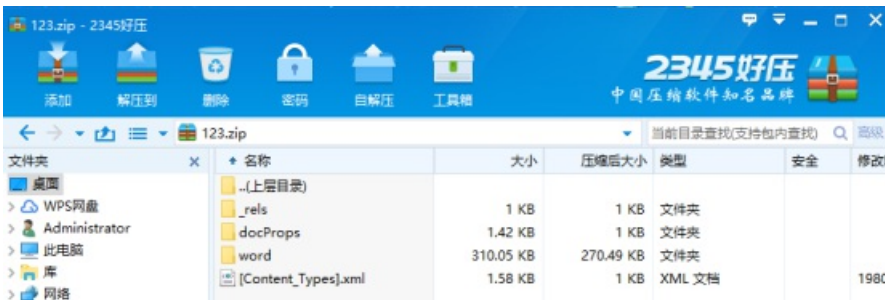


这里的docx本萌新实在是弄不出来，

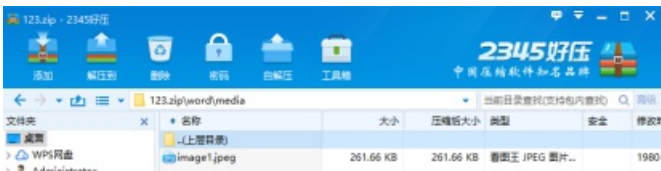
只能另辟蹊径，于是乎继续查资料，当看到这句“word文档其本质就是一个压缩包。”时，啊，我感觉我又有了救了，果断保存为123.zip

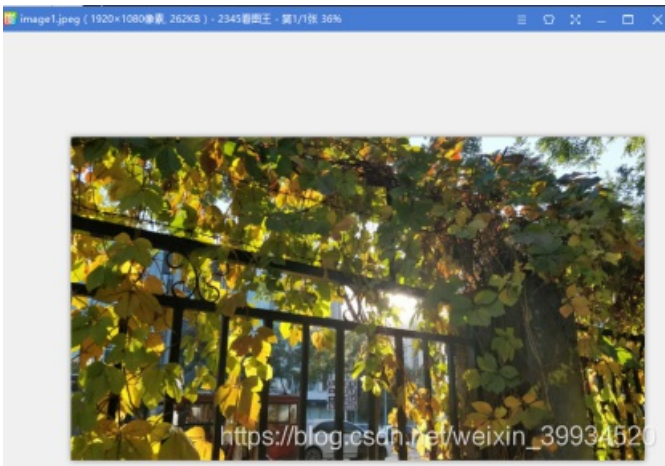


查看，发现一大堆东西：



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)

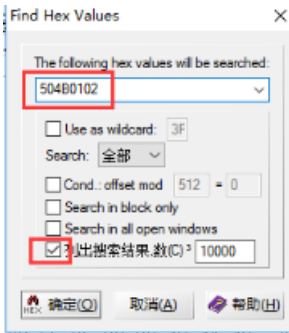
3F 00：压缩使用的 pkware 版本

14 00：解压文件所需 pkware 版本

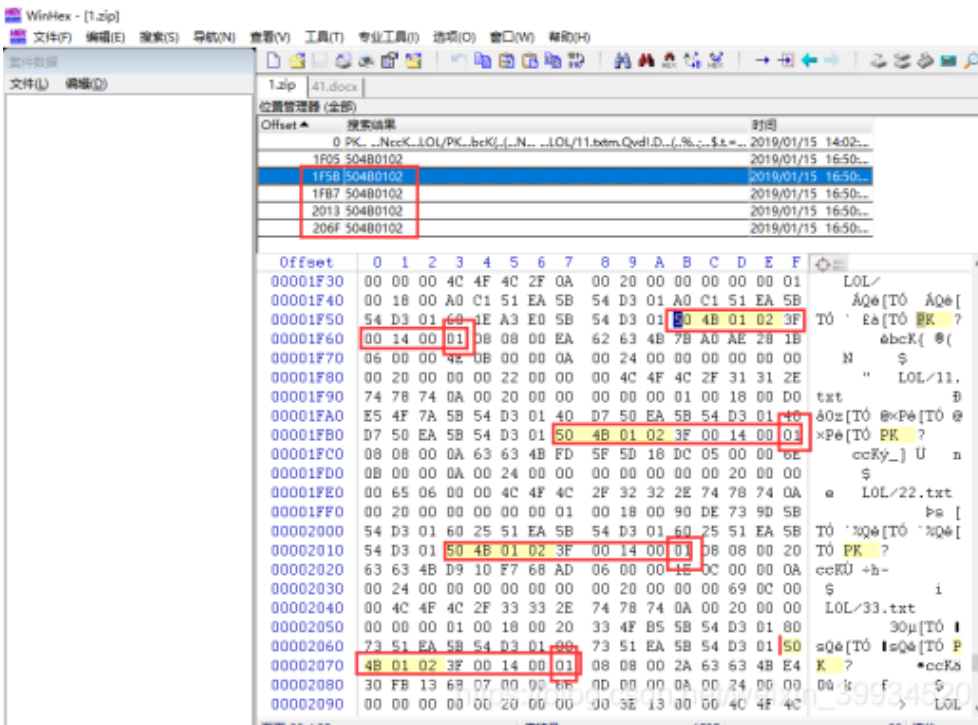
00 00：全局方式位标记（有无加密，偶加奇不加）

伪加密的特征，奇数结尾。

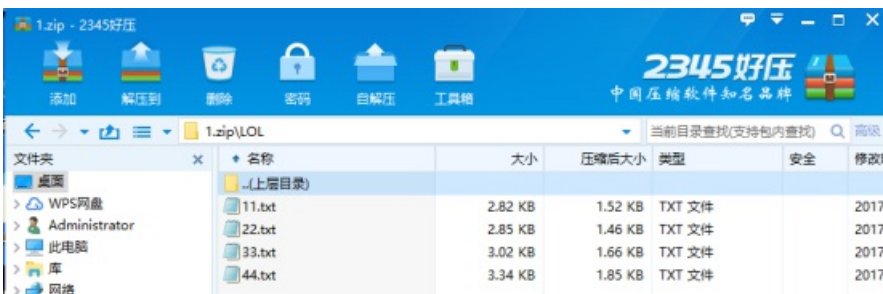
搜索压缩源文件目录区：



4个文档:



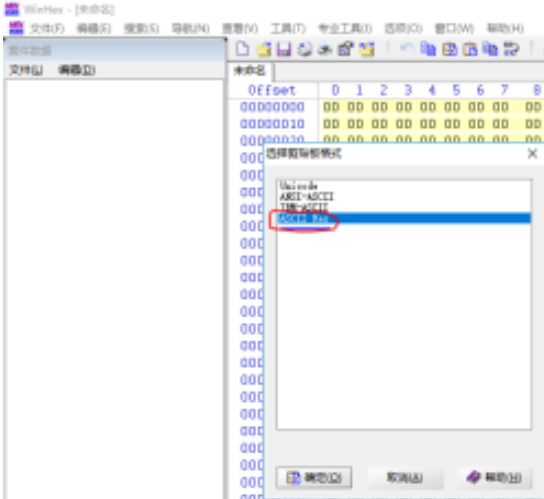
把奇数1可以改为偶数2，保存并打开:



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ASCII HEX形式，然后保存：



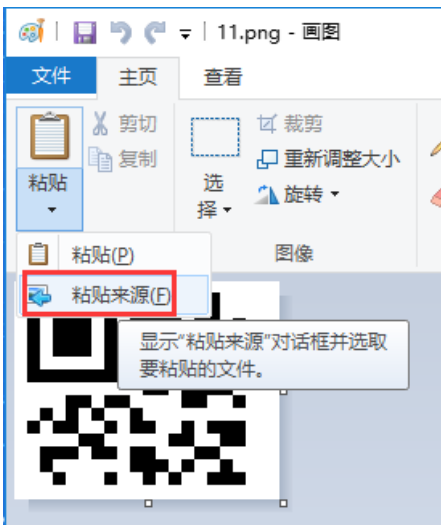
很明显这四个应该能和成一个正常的二维码：

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

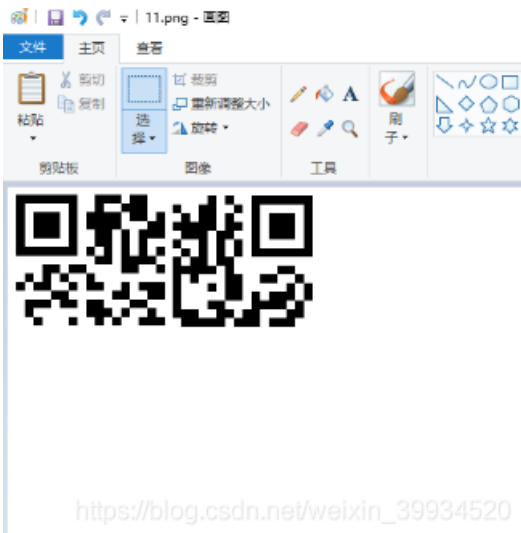
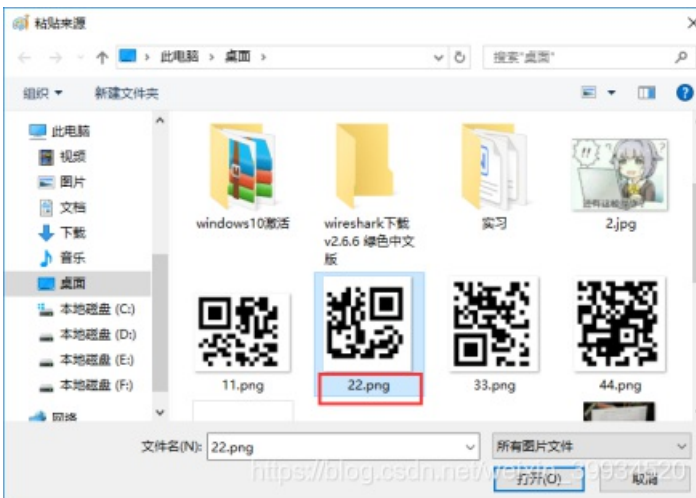
于是乎，画图神器出来了。。。

来画图工具走起：

先打开11.png再选择粘贴来源



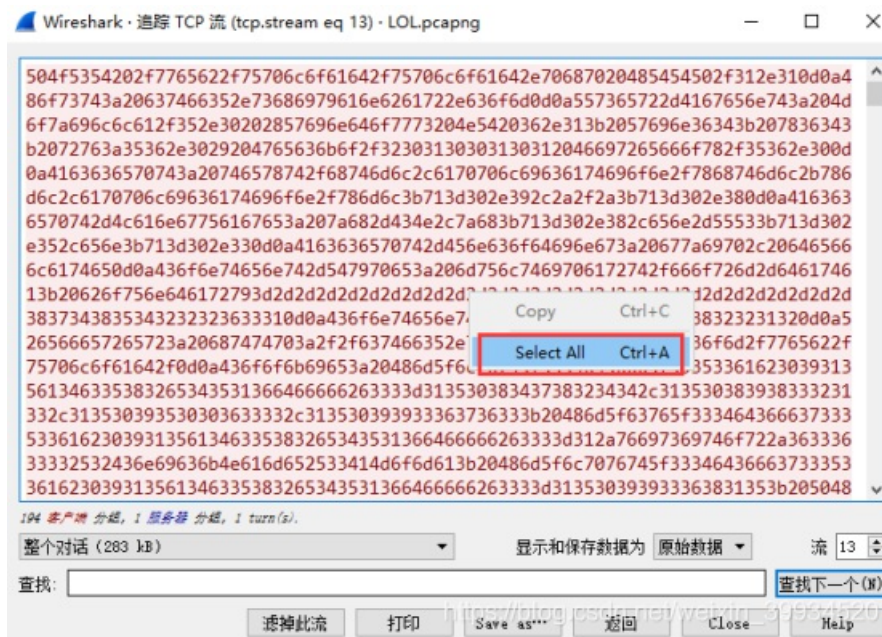
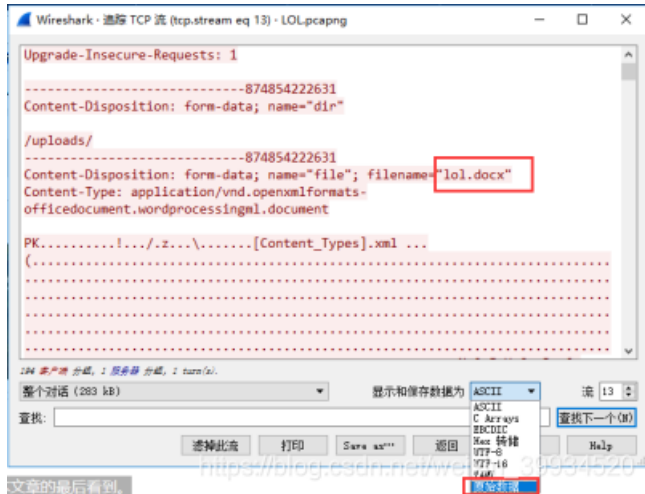
然后选择另一张图片22.png



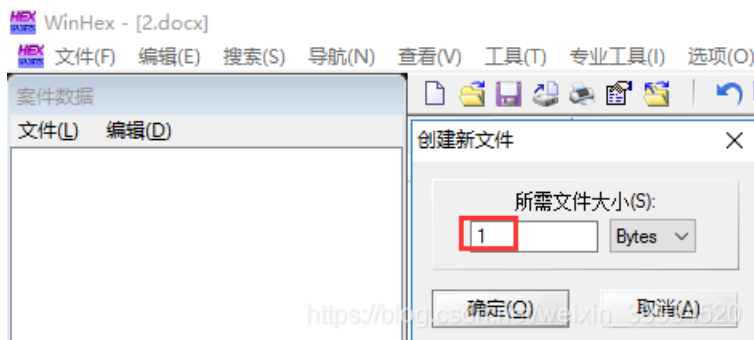
继续。。。

##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


```

Offset  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
00000000  48 03 04 14 00 06 00 08 00 00 00 21 00 0E D7
00000016  2F 99 7A 01 00 00 0C 0A 00 00 13 00 08 02 58 43
00000032  6F 6E 74 65 6E 74 6F 64 79 70 65 73 02 7E 6D
00000048  6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00
00000064  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000096  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000112  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000128  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000144  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000176  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000192  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000208  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000224  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000240  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000256  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000272  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000288  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000304  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000336  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000352  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000368  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000384  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000416  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000432  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000448  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000464  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000480  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

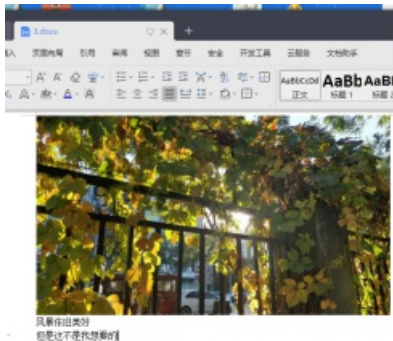
然后，把该文件的底部，PKI后面的都删除

```

Offset  0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
00281424  73 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08
00281440  00 00 00 21 00 81 56 46 27 14 02 00 00 10 06 00
00281456  00 12 00 00 00 00 00 00 00 00 00 00 00 00 00 F7
00281472  33 04 00 77 6F 72 64 2F 66 6F 6E 74 54 61 62 6C
00281488  65 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08
00281504  00 00 00 21 00 5B 60 FD 93 09 01 00 00 F1 01 00
00281520  00 14 00 00 00 00 00 00 00 00 00 00 00 00 00 3B
00281536  36 04 00 77 6F 72 64 2F 77 65 62 53 65 74 74 69
00281552  6E 67 73 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06
00281568  00 08 00 00 00 21 00 4D 40 BC C3 73 03 00 00 D0
00281584  02 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00
00281600  00 76 37 04 00 64 6F 63 50 72 6E 70 73 2F 61 70
00281616  70 2E 78 6D 6C 50 4B 01 02 2D 00 14 00 06 00 08
00281632  00 00 00 21 00 01 2A 0E A0 21 0C 00 00 37 75 00
00281648  00 0F 00 00 00 00 00 00 00 00 00 00 00 00 00 1F
00281664  3A 04 00 77 6F 72 64 2F 73 74 79 6C 65 73 2E 78
00281680  6D 6C 50 4B 01 02 2D 00 14 00 06 00 08 00 00 00
00281696  21 00 FD 02 30 DA 69 01 00 00 DF 02 00 00 13 00
00281712  00 00 00 00 00 00 00 00 00 00 00 00 00 46 04 00
00281728  64 6F 63 50 72 6F 70 73 2F 63 6F 72 65 2E 78 6D
00281744  6C 50 4B 03 06 0C 0C 00 0E 00 0E 00 84 03 00
00281760  00 0D 49 04 00 00 00 00

```

然后，保存为3.docx并打开：



补：其实删除的都是这些内容：

```

POST /web/uploads/upload.php HTTP/1.1
Host: ctfs.shiyandar.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----874854222631
Content-Length: 282212
Referer: http://ctfs.shiyandar.com/web/uploads/
Cookie: Hm_lvt_34d6f7353ab8915ad582e4516dfbc3=1508478244,1508983213,1509508633,1509936763;
Hm_cv_34d6f7353ab8915ad582e4516dfbc3=1*visitor*6363382CnickNameX3APoma;
Hm_lpv_34d6f7353ab8915ad582e4516dfbc3=1509936815; PHPSESSID=up66htf11qf01e159e0118sq0
X-Forwarded-For: 192.168.200.126
Connection: keep-alive
Upgrade-Insecure-Requests: 1
-----874854222631
Content-Disposition: form-data; name="dl"
/uploads/
-----874854222631
Content-Disposition: form-data; name="file"; filename="lol.docx"
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

PK.....[Content_Types].xml ...

```

```
Wireshark - 跟踪 TCP 流 (tcp.stream eq 13) - LOLpcapng
-----874854222631
Content-Disposition: form-data; name="submit"

Submit
-----874854222631--
HTTP/1.1 200 OK
Date: Mon, 06 Nov 2017 02:58:29 GMT
Server: Apache/2.4.18 (Win32) OpenSSL/1.0.2e PHP/5.2.17
X-Powered-By: PHP/5.2.17
Content-Length: 119
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<html><head><meta charset="utf-8" /></head><body>
.....jpg,gif,png.....
```



[创作打卡挑战赛](#)
赢取流量/现金/CSDN周边激励大奖