欢迎来到地狱 WriteUp（2019暑假CTF第一周misc）

转载

afu42832 于 2019-07-09 10:44:00 发布 197 收藏
文章标签： php photoshop
原文链接：http://www.cnblogs.com/hardcoreYutian/p/11155774.html
版权
目录

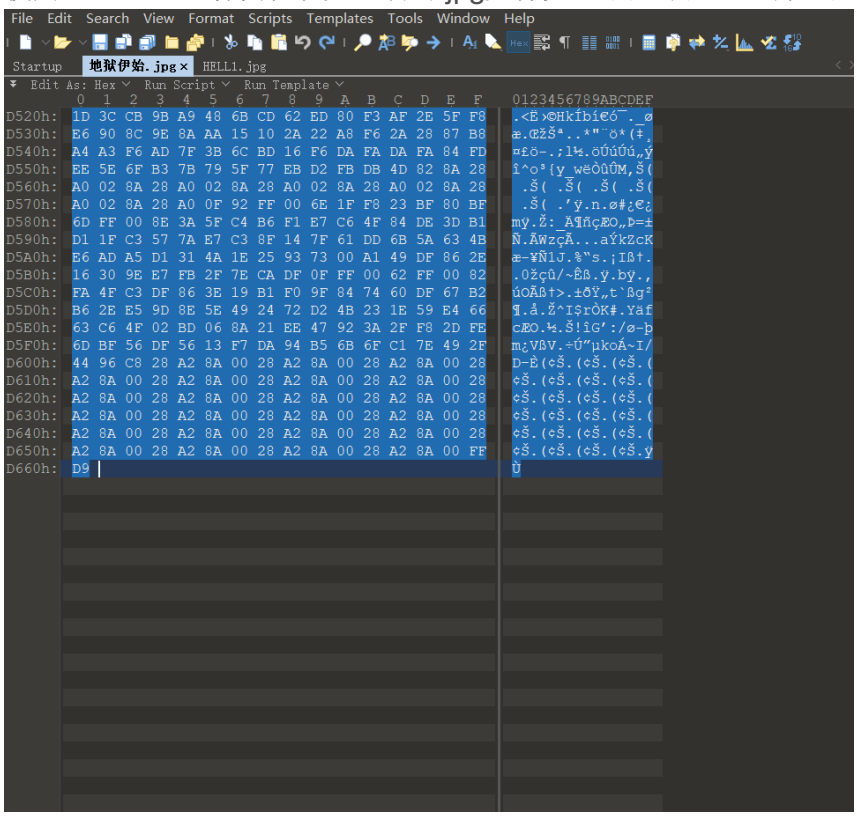
0707，0708，0709

题目地址：欢迎来到地狱

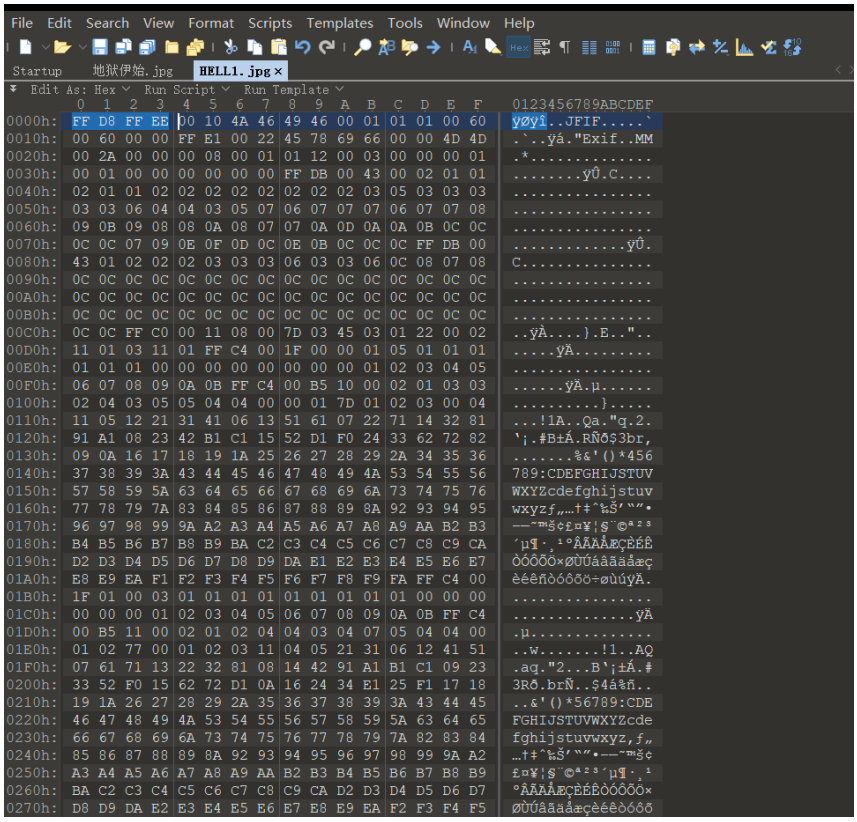
下载下来有3个文件，地狱伊始.jpg，第二层地狱.wav，快到终点了.zip。依次解之。

1.地狱伊始.jpg

使用hexeditor查看发现缺少正确的.jpg文件头，于是添加之。方法是先复制全部



然后新建Hex文件，敲入FFD8FFE0，再把复制的内容粘进去



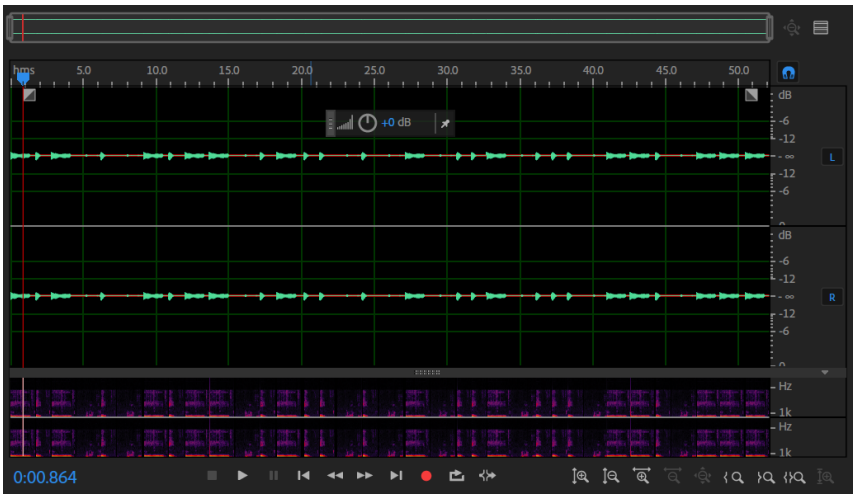
保存为.jpg文件，就可以正常打开了。

很久很久以前，有一位。。。。。。。。小姐姐。。。。。。。。扑通一下子。。。。。。。。掉进了地狱。（别问我为啥，因为她沉行不行）。。。。。。总之。。。。有一位河神有一天对你说："年轻的樵夫呀，你掉的是这个小姐姐呢，还是。。。。。。总之你快去救她吧！"对了，我这里有盘盘的资源呦！

http://pan.baidu.com/s/1i49Thlj

打开图片，复制里面的网盘链接，下载下来是一个.wav文件。

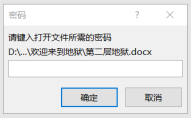
1.5地狱之声.wav



用au打开，查看频率部分，由一长一短两种固定长短的线条组成，可联想到摩斯码。

翻译得keyletusgo。

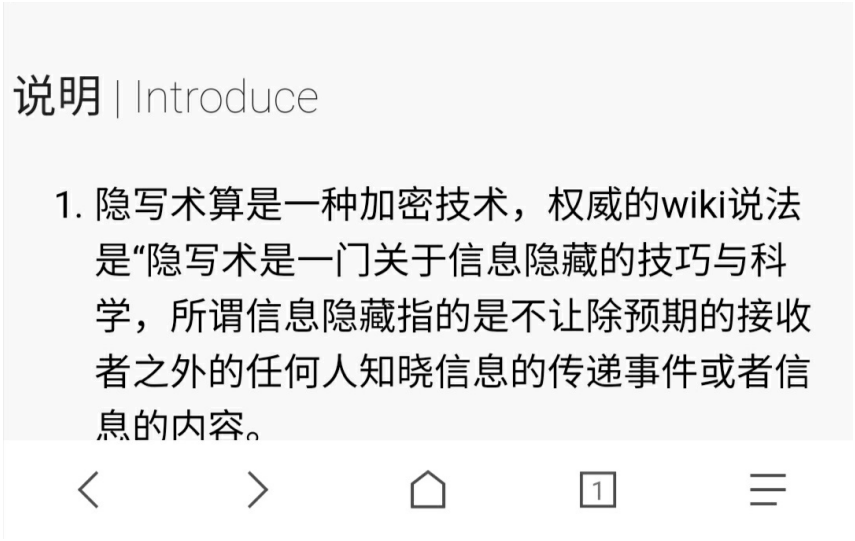
2.第二层地狱.docx



需要输入密码打开，我们输入用地狱之声解出来的lesusgo

在word中文件>>选项>>显示，勾选“隐藏文字”

发现多了一句话：image steganography，是图片隐写。
搜索之找到一个在线网站image steganography，虽然解不了本题，但是码一下吧。
然后我又下载了一个叫image steganography的软件，还是解不了。
网上说使用在线网站：http://www.atool.org/steganography.php 可以解，但是我的电脑打不开这个网址。
用手机就能打开了。顺便贴一下其代码参考地址： https://github.com/oakes/PixelJihad
但是手机解不了。

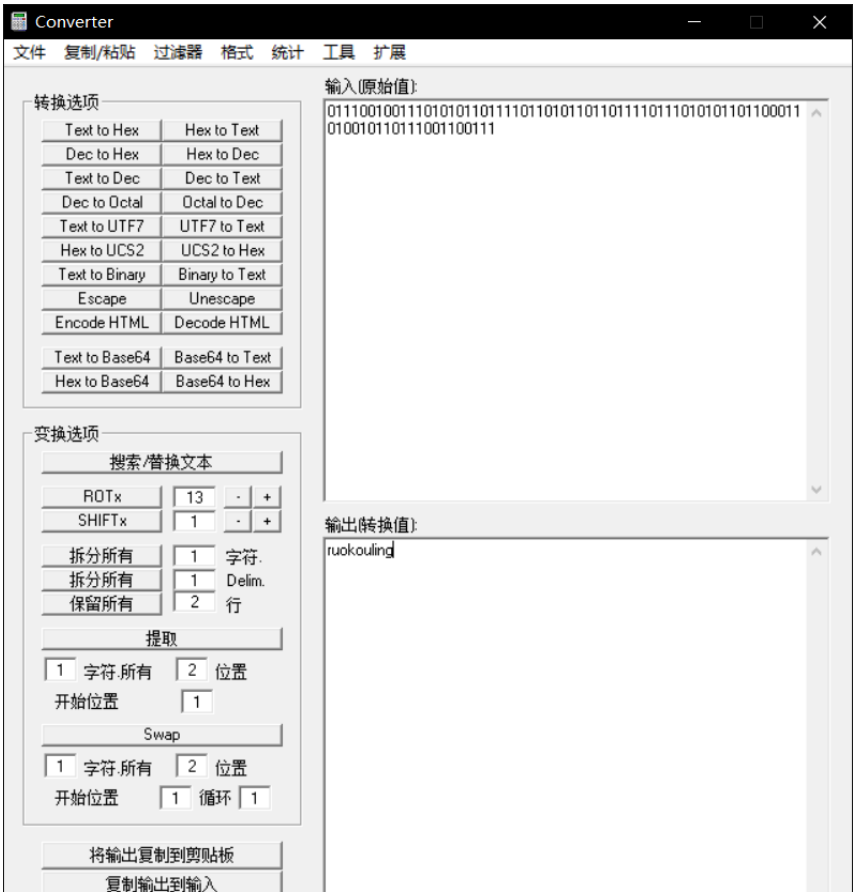


这时候我奇思妙想，用手机给电脑开热点，然后就能用电脑进入这个网址了。

不容易不容易啊。得到key{you are in finally hell now}

3.快到终点了.zip

解压之发现需要密码，输入you are in finally hell now，解压。
解压出来有一个图片和一个文本文件，文本文件里面是一串01串，使用converter转成text发现是ruokouling，也就是弱口令的拼音。



在kali中对图片“地狱大门.jpg”使用binwalk，发现藏了个.zip文件，用dd分离出来。

```
root@yutianhack:/mnt/hgfs/yutianhackshare/CTF培训作业/欢迎来到地狱/快到终点了# binwalk
地狱大门.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
62584         0xF478          End of Zip archive, footer length: 22

root@yutianhack:/mnt/hgfs/yutianhackshare/CTF培训作业/欢迎来到地狱/快到终点了# dd if=地
狱大门.jpg of=开门.zip skip=62584 bs=1
记录了22+0 的读入
记录了22+0 的写出
22 bytes copied, 0.00705583 s, 3.1 kB/s
root@yutianhack:/mnt/hgfs/yutianhackshare/CTF培训作业/欢迎来到地狱/快到终点了# ls
地狱大门.jpg  开门.zip  最后一层地狱.txt
```

发现这个.zip文件坏了，解压不了。

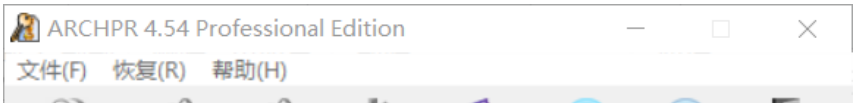
用winhex改其文件头为504B0304，在文件尾部添加50 4B进行修复。

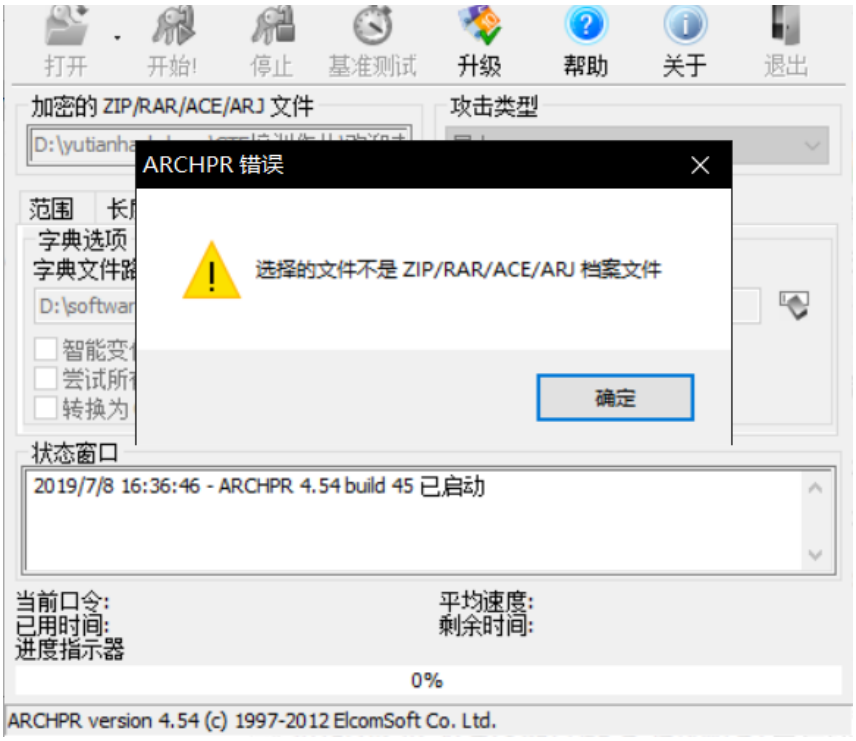
然后发现还是显示损坏。

整这么多花里胡哨的无果，其实改一下后缀名就能解决。。

然后要输入密码，所以根据弱口令的提示，我们进行弱口令爆破就可以了。

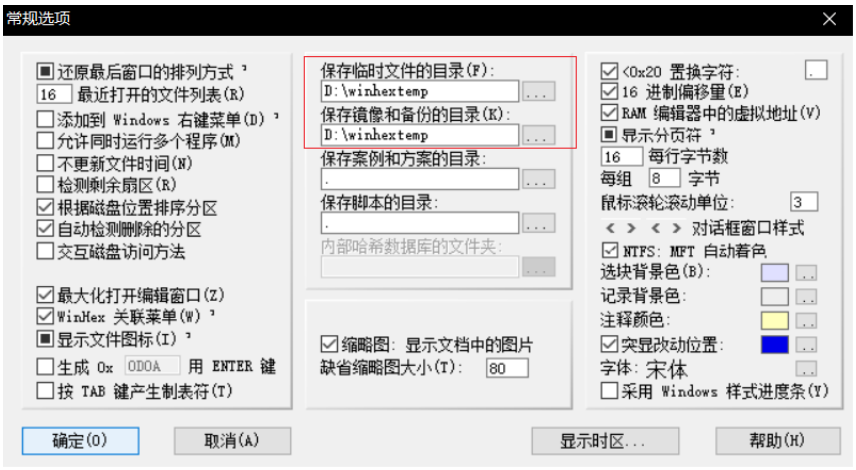
爆破发现不是.zip文件，所以应该这个时候修改文件头才对（多谢马老师指点）。





结果修改后保存显示“请确信文件夹存在和文件未被写保护”的错误。

然后在选项>>常规，修改临时文件目录和保存镜像和备份的目录为一个我自己建的目录，点确定后退出winhex。

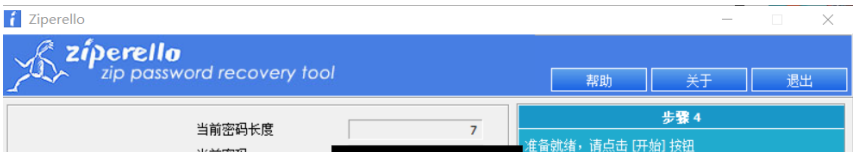


见鬼的是再次打开winhex后发现这两个目录竟然没有变化。

尝试半天无果我决定去它的，用010editor吧。

然后还是各种失败，，，好吧，换一个破解工具ziperello。

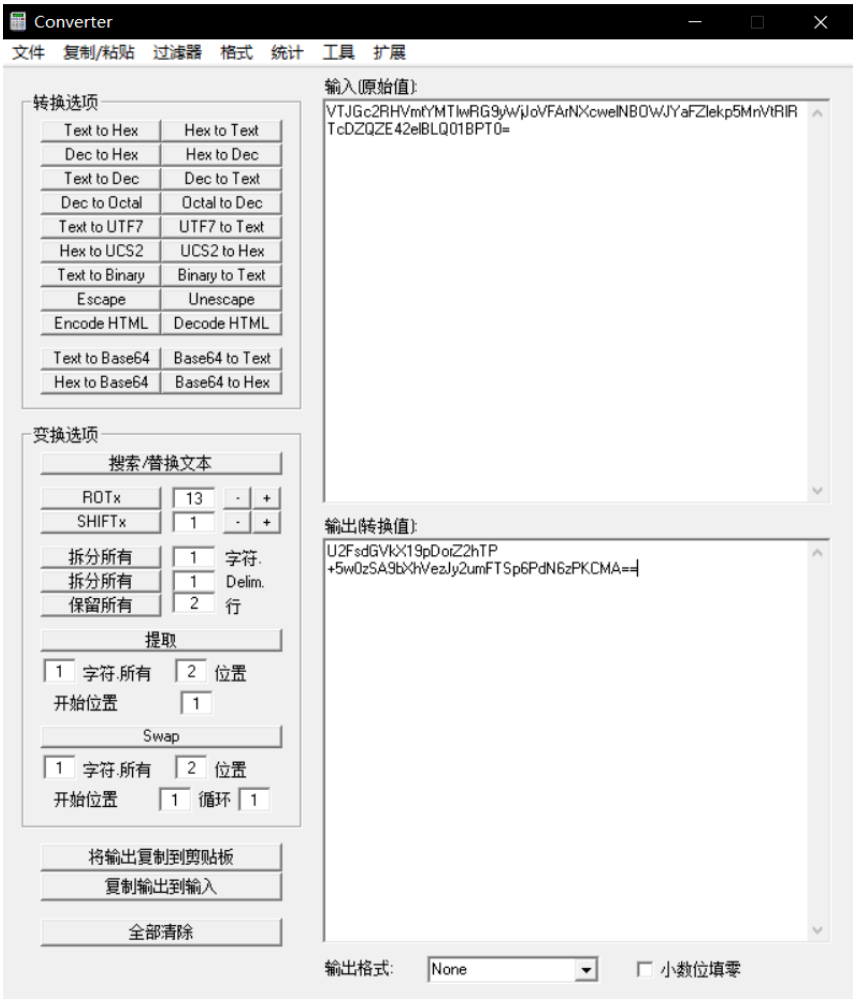
暴力破解48小时都搞不完，我破了几个小时后想了想放弃了，改成用字典破，结果第二个字典就秒出了。



输入密码，解压出来是这样一个文本文件（我手动换行了，方便观看）

可见是一个连环加密，我们要解密需要按与加密时相反的顺序，所以先base64（贝斯、sixfour），再rabbit解密（兔子洞穴），再凯撒密码（凯撒家族）。

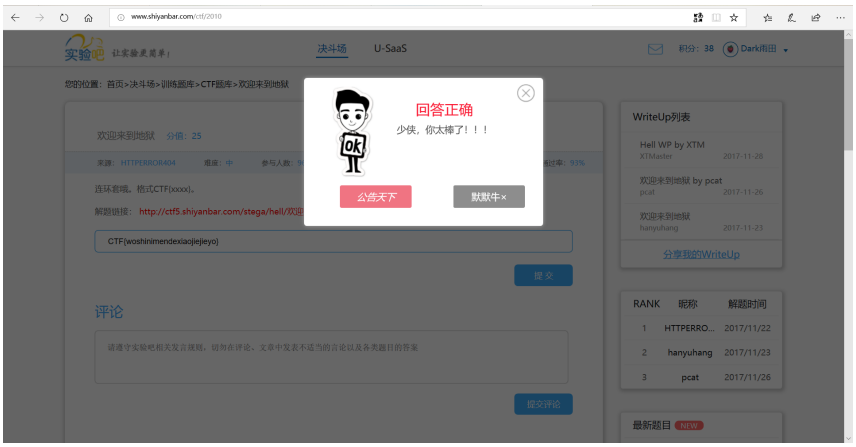
base64转文本：



rabbit解密：

凯撒加密，一个一个偏移值的试，试到17时发现是一句拼音“我是你们的小姐姐哟”

提交之，本题完成。



参考

1.码一下常见的文件头：
常用文件的文件头如下(16进制)：
JPEG (jpg)，文件头：FFD8FFE0或FFD8FFE1或FFD8FFE8
GIF (gif)，文件头：47494638PNG (png)，文件头：89504E47
TIFF (tif)，文件头：49492A00
Windows Bitmap (bmp)，文件头：424DC001
CAD (dwg)，文件头：41433130
Adobe Photoshop (psd)，文件头：38425053
Rich Text Format (rtf)，文件头：7B5C727466
XML (xml)，文件头：3C3F786D6C
HTML (html)，文件头：68746D6C3E
Email [thorough only] (eml)，文件头：44656C69766572792D646174653A
Outlook Express (dbx)，文件头：CFAD12FEC5FD746F
Outlook (pst)，文件头：2142444E
MS Word/Excel (xls.or.doc)，文件头：D0CF11E0
MS Access (mdb)，文件头：5374616E64617264204A
WordPerfect (wpd)，文件头：FF575043
Adobe Acrobat (pdf)，文件头：255044462D312E
Quicken (qdf)，文件头：AC9EBD8F
Windows Password (pwl)，文件头：E3828596
ZIP Archive (zip)，文件头：504B0304
RAR Archive (rar)，文件头：52617221
Wave (wav)，文件头：57415645
AVI (avi)，文件头：41564920
Real Audio (ram)，文件头：2E7261FD
Real Media (rm)，文件头：2E524D46
MPEG (mpg)，文件头：000001BA
MPEG (mpg)，文件头：000001B3
Quicktime (mov)，文件头：6D6F6F76
Windows Media (asf)，文件头：3026B2758E66CF11
MIDI (mid)，文件头：4D546864

还有一个含文件尾的：文件头文件尾总结

2.凯撒加密
3.rabbit解密

转载于:https://www.cnblogs.com/hardcoreYutian/p/11155774.html