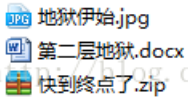
【网安随笔】CTF-writeup -环环相扣的隐写

原创

Keyli0n 于 2017-12-06 21:38:05 发布 1217 收藏 2
分类专栏： 网络安全杂谈

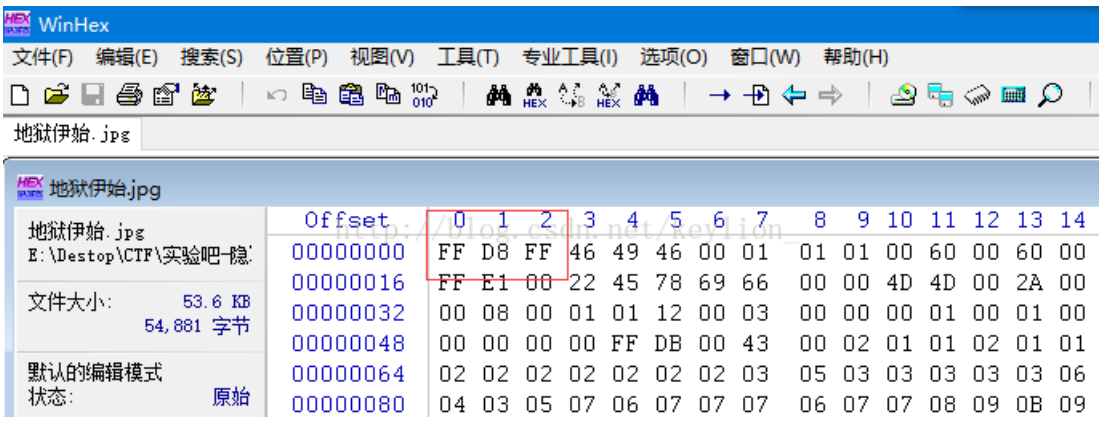
本文链接：https://blog.csdn.net/keylion_/article/details/78735045



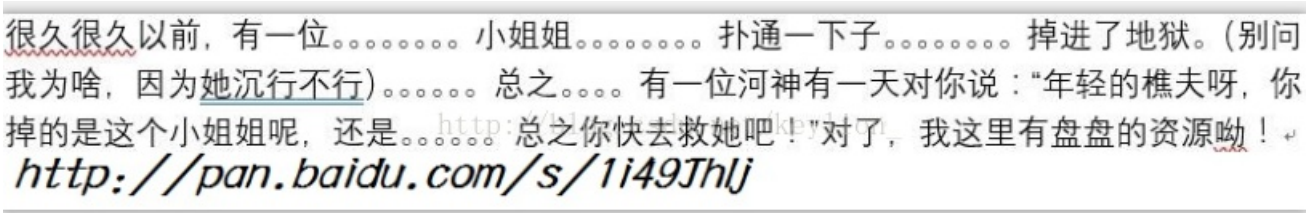
这是我们这次要破解的源文件。把三个文件都点开看下，发现文档和压缩包都是加密的。正常思路：第一个jpg文件里隐藏了，docx文件的密码，从docx文件里获取压缩包的密码，最后得到flag.

一、地狱伊始.jpg

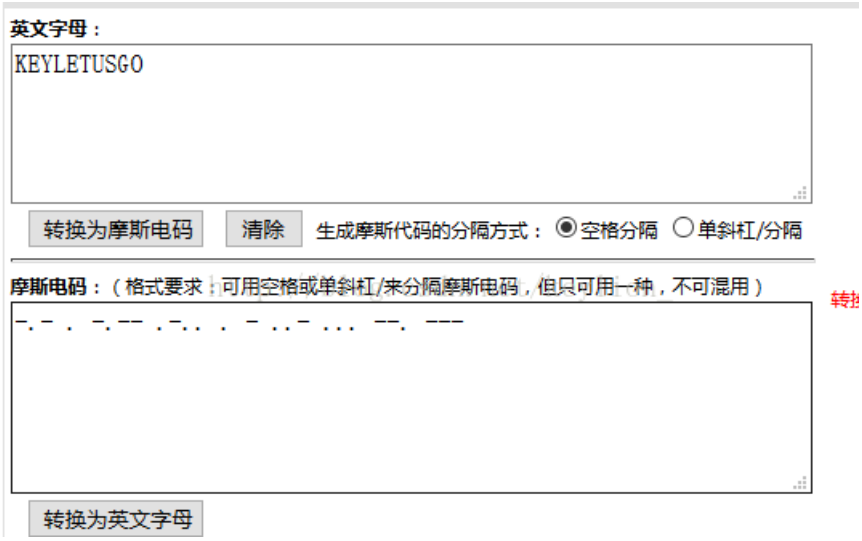
直接打开发现图形是不显示的，所以要用Winhex去尝试修复，打开文件发现果然文件头是损坏的，这里普及下芝士，jpg的文件头：FF D8 FF



修复保存，然后就可以打开了。



出题人又抛给一个链接，按照链接下载是一个wav音频文件。仔细听，很明显是莫尔斯加密。整理出来。解密



二、第二层地狱

得到KEY 的值是LETUSGO, 当我们兴高采烈的去试那个文档时发现还是打不开，其实是小写的letusgo, 噗,只能说出题人够蛋疼。

习惯性的想到word隐写，打开word中的隐藏文字功能就可以了。word2010打开路径是：文件->选项->显示->隐藏文字

你现在在第二层地狱中，凶猛的。。。。额。。。。哈士奇。。。。。把守着通向第三层地狱的钥匙，那么。。。。。。。。。你要用你手中的剑（握草，老子剑呢，

image steganography，，，是不是掉在第二层地狱的哪里了）

按照提示（一个很常见的image加密解密工具）发现，本地的工具不起作用，好吧，那就用web版的。链接抛给你：
image steganography web版 http://www.atool.org/steganography.php
发现解密成功。

二、、解密带隐藏信息的图片

1. 从电脑中选择一张带有隐藏信息的图片： 浏览... aaa.png

2. 输入需要解开信息的密码（如果没有密码可以不填）： 信息查看密码，可以为空即为图片解密不需要密码

解密出隐藏的信息

图片中隐藏的信息为：key{you are in finally hell now}

得到压缩包的解压密码。you are in finally hell now

三、快到终点了

解压缩：得到两个新文件。

打开TXT文件：

常见的二进制转ASCII编码，8位一组，正好十组。解密如下：

（tips：　　01110010 01110101 01101111 01101011 01101111 01110101 01101100 01101001 01101110 01100111 ）

转化为十进制：　114　117　111　107　111　117　108　105　110　103

对应ASC表 ：　r　u　o　k　o　u　l　i　n　g

密码：　roukouling

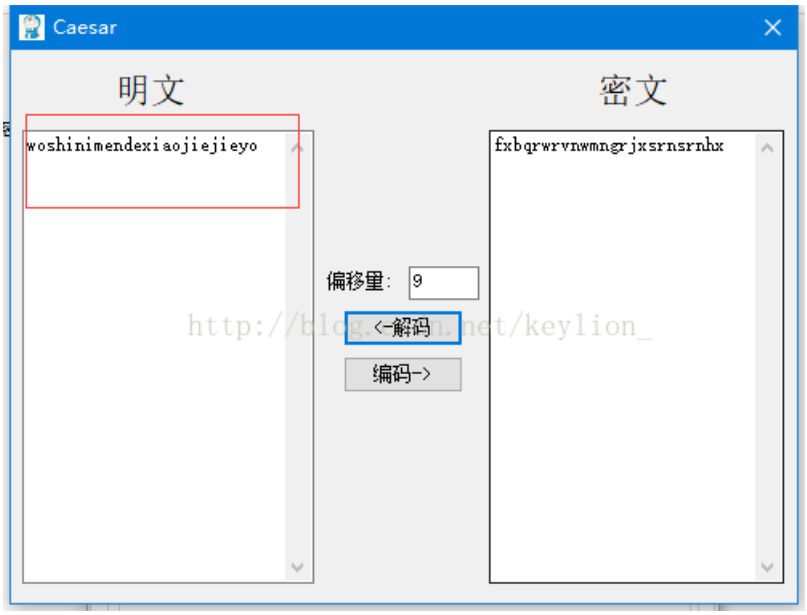
这个密码用在哪里呢？按照前面的思路，jpg文件可能也是一个隐藏的压缩包。把文件后缀改成rar，发现可以打开。但是加密的。

既然提示是密码是弱口令那么常见的密码都试试，password,Possword,12345。用字典扫下就可以出来。密码是Password.

解压后

给的这段信息，整理下的密文就是经过凯撒加密、rabbit加密、Base64加密后的字符串。所以逆向导过去就是flag.

这里特殊说一下凯撒密码的偏移量是9,flag出现。



给出源文件地址：链接：链接：https://pan.baidu.com/s/1pK8nMbD 密码：7big