地狱来了（JPG的隐写）

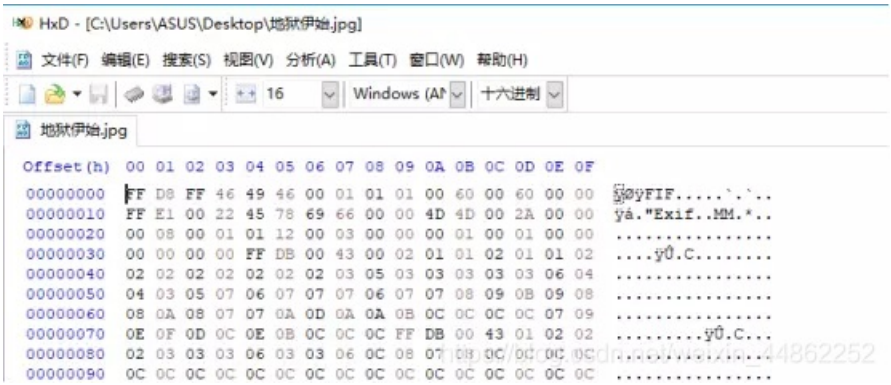
原创

weixin_44862252 于 2019-09-05 22:41:08 发布 761 收藏 3

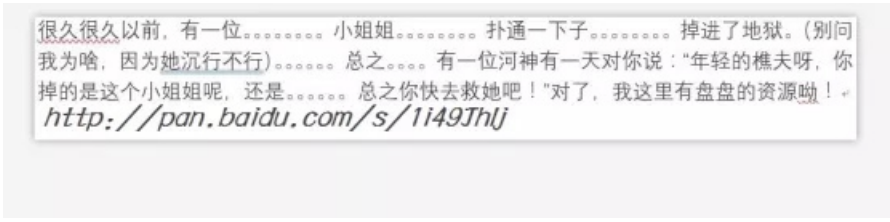
地狱来了（JPG的隐写）

第一步：我们需要理解几种格式的开头（就是放在HXDX64.EXE中的开头）JPG的开头是：FFD8FF

第二步：我们就是要把一张不能打开的图片进行修护，就用到了HXDX64.EXE的软件，将图片放到HXDX64.EXE中，可以发现JPG的开头不是(FF D8 FF),这时就要将开头变成（FF D8 FF)在进行保存

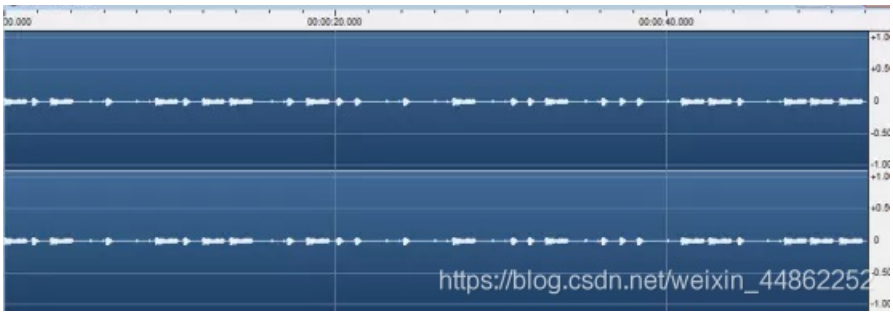


再打开我们可以发现有一些汉字和一个网址。

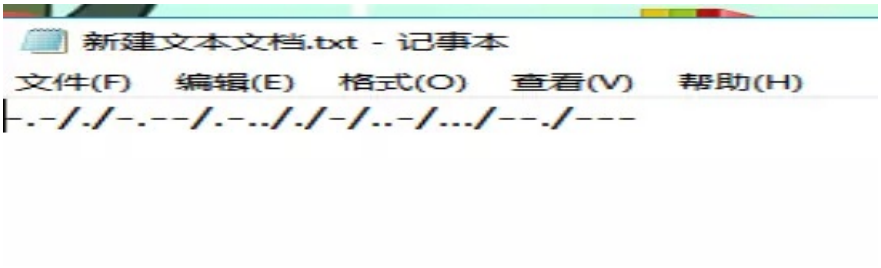


而这个网址就比较的可疑，所以我们按这个网址的信息一步一步走。可以知道需要下载一段音频（WAR).然后就百度知道是莫尔斯密码，就百度莫尔斯密码的原理，是以(. - /)构成的

再通过将wav转化为我们能够看懂的图形。如下



转化莫尔斯密码如下：



再从百度上搜索将莫尔斯密码转化为子符为

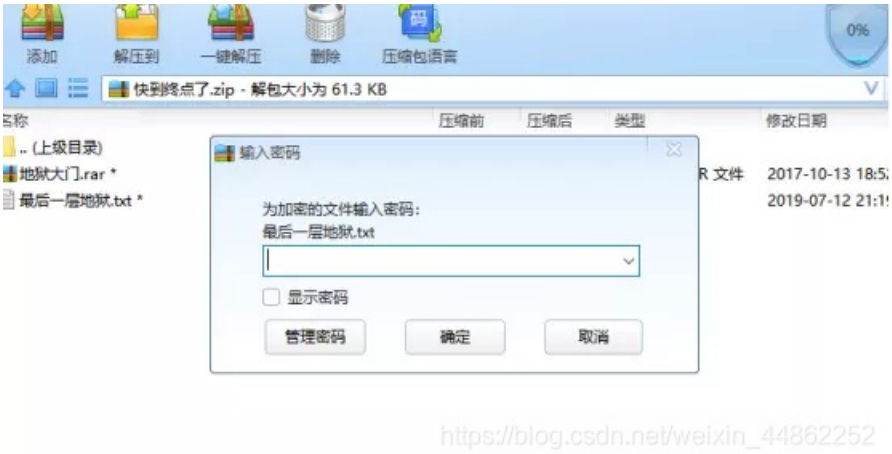
可见密码为{LETUSGO}这就是第二层的密码，输入后大写打不开，那就试试小写，打开了。打开可以看见是一个word文档里面有一张图片和文字，显然图片很可疑。

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，是不是掉在第二层地狱的哪里了）
但也看不出啥东西。我就问了赵志豪他说是word文档的隐写，他帮我操作了一番。具体步骤是打开文件–选项–工具–隐藏文字。然后发现多出了（image steganography，，，），之后百度发现是图片隐写。所以就要研究这张哈士奇了。

接下来我就不会了。看别人的博客也知道咋把图片隐写破解这个里用到一个脚本

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

输入到下面解开后出现了一个文档

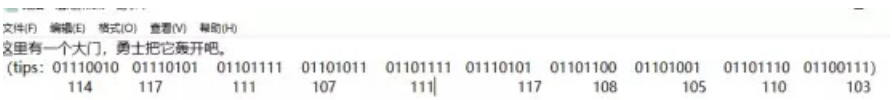


然后内心是崩溃的然后打开最后一层地狱

可以看出是一串二进制代码这就是解开小姐姐的密码但是如何转化为我们想要的密码呢？仔细观察看出每八位一组正好，就可以看出是八进制代码。

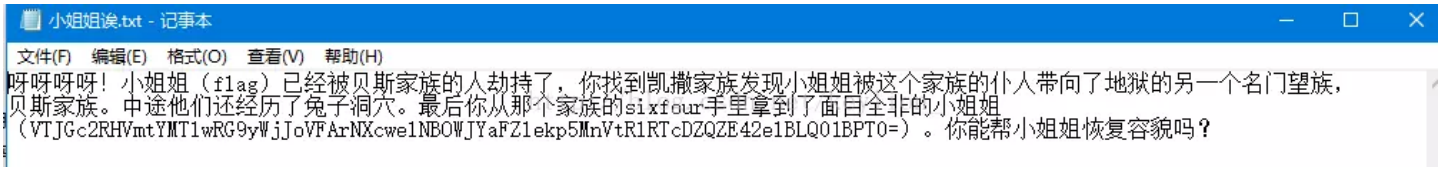
然后就想不到，就看了网上的博客，将八进制转化为十进制后在一一对应数值所对应的ASll码。这一样就能够得到我们想要的信息了。

但是我在转化进制的时候出现了和大佬不一样的结果。



这就是打开小姐姐的密码

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。

总结
关于JPG隐写的总结

1.当图片不能看时需要你将图片放到HXDX64.EXE软件中（在这里你需要了解一些文件的开头如下）

2. Jpg开头为FF D8 FF

3.Word文档也可以隐藏信息

4. 图片中也可以隐藏信息。

各种密码的特点

base64特点：

编码后的字符串的长度一定会被4整除，包括用作后缀的等号吧；如果明文字符数不能被3整除，余1时，1个字符转为2个，补2个等号，共4个字符；余2时，2个字符转为3个字符，补1个等号，共4个字符；其实归根结底就是一句话：经过base64编码后的字符串长度一定会被4整除（包括后缀等号）

1.标准base64只有64个字符（英文大小写、数字和+、/）以及用作后缀等号；

2.base64是把3个字节变成4个可打印字符，所以base64编码后的字符串一定能被4整除（不算用作后缀的等号）；

3.等号一定用作后缀，且数目一定是0个、1个或2个。这是因为如果原文长度不能被3整除，base64要在后面添加\0凑齐3n位。为了正确还原，添加了几个\0就加上几个等号。显然添加等号的数目只能是0、1或2；

4.严格来说base64不能算是一种加密，只能说是编码转换。使用base64的初衷。是为了方便把含有不可见字符串的信息用可见字符串表示出来，以便复制粘贴；

Base32和Base64的一点区分注意
看到编码内容，只有大写和数字，根据Base64和Base32 区别：base64中包含大写字母（A-Z）、小写字母（a-z）、数字0——9以及+/； base32中只有大写字母（A-Z）和数字234567 使用base32编码解码：
GUYDIMZVGQ2DMN3CGRQTONJXGM3TINLGG42DGMZXGM3TINLGGY4DGNBXGYZTGNLGGY3DGNBWMU3WI===
得:504354467b4a7573745f743373745f683476335f66346e7d然后16进制编码得到flag

1.简单的数字例如：8888888 111111111 123456

简单的字母例如：Password,abcd等

或者两个结合

总之就是比较简单的密码、

一般用在你不知道密码咋解，完全没有任何信息。

凯撒密码

凯撒密码一般指恺撒密码

它是一种代换密码。据说凯撒是率先使用加密函的古代将领之一，因此这种加密方法被称为凯撒密码。

凯撒密码作为一种最为古老的对称加密体制，在古罗马的时候都已经很流行，他的基本思想是：通过把字母移动一定的位数来实现加密和解密。明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推X将变成A，Y变成B，Z变成C。由此可见，位数就是凯撒密码加密和解密的密钥。

概念

在密码学中，凯撒密码（或称恺撒加密、恺撒变换、变换加密）是一种最简单且最广为人知的加密技术。它是一种替换加密的技术。这个加密方法是以恺撒的名字命名的，当年恺撒曾用此方法与其将军们进行联系。恺撒密码通常被作为其他更复杂的加密方法中的一个步骤，例如维吉尼亚密码。恺撒密码还在现代的ROT13系统中被应用。但是和所有的利用字母表进行替换的加密技术一样，恺撒密码非常容易被破解，而且在实际应用中也无法保证通信安全。