实验吧关于隐写术的writeUp（一）

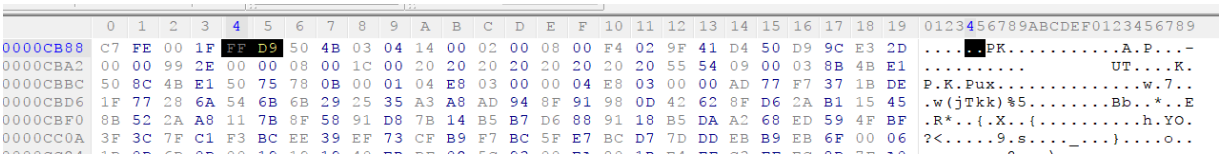
转载

weixin_34128237 于 2017-10-07 19:45:00 发布 475 收藏
原文链接：http://www.cnblogs.com/Triomphe/p/7635591.html

0x01 Spamcarver

原题链接 http://www.shiyanbar.com/ctf/2002

1.用Hex workshop打开图片，图片的开头是 FF D8 ，这是jpeg格式的文件头。相应的，寻找 FF D9（jpeg文件尾）



2.在文件的下半部分找到了FF D9，在后面跟的是pk，这是zip压缩文件格式的开头，说明后面追加了一个zip文件。注：**pk是zip压缩文件发明者的名字首字母**

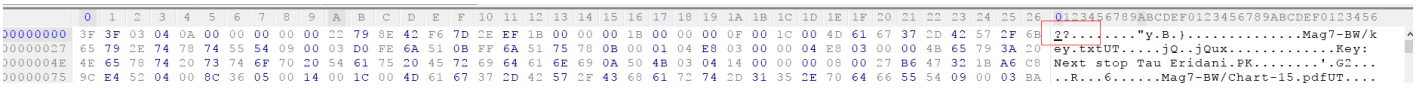
3.用 foremost（命令行工具）提取文件，得到zip文件，解压得到flag图片

0x02 NAVSAT

原题链接 http://www.shiyanbar.com/ctf/2001

1.下载文件后是一个zip，先解压发现解压出错。 而题目提示缝缝补补又三年。 得出，可能要补全文件的校验位置

2.用hex workshop 打开文件，文件头错误。应该是pk



3修改文件头，正常解压，得到flag

0x03 In Hex, No One Can Hear You Complain

原题链接 http://www.shiyanbar.com/ctf/2000

1.打开docx文件出错。用hex workshop打开，发现文件头为pk，修改文件格式为zip格式

2.解压得到文件夹

3,在文件夹中得到flag图片

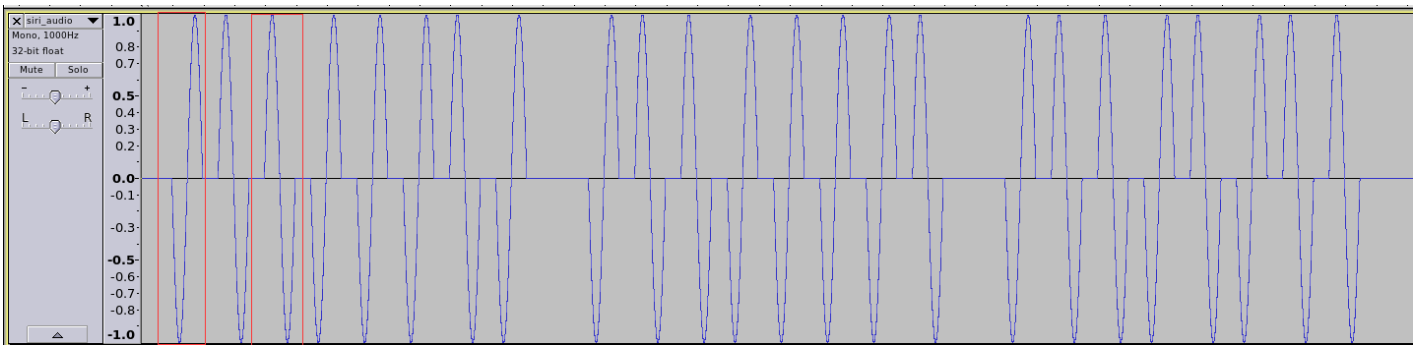
KEY:
docx_why_not_docz

0x04 stegas 300

原题链接 http://www.shiyanbar.com/ctf/1999

1.题目给出的提示是分析音频波形，先下载，发现是一段wav格式的音频。

2.用**audacity**软件进行音频分析



3.在软件中可以得到音频图像。图像分为两种：**先向下再向上**和**先向上再向下**（已经用红线标出）。而8个这样的图像中间就会有间隔。可以从中猜到应该是表示0和1然后8位组成一个ascii码。

假设 **下上为 0 上下为 1**

01100010 01100001 01101011 01100100 01101111 01110010 因为开头都是0，所以假设应该成立，转换成字母得到**bakdor**

3.这个题目给的有问题，我找到了最初的题目，最后有一句意思是字母的md5值就是key。 然后把**bakdor**的MD5值算出来，提交正确

0x05 越光宝盒

原题链接： http://www.shiyanbar.com/ctf/1992

解题链接：http://www.cnblogs.com/Triomphe/p/7581625.html

0x06 Dark Star

， 原题链接：http://www.shiyanbar.com/ctf/1989

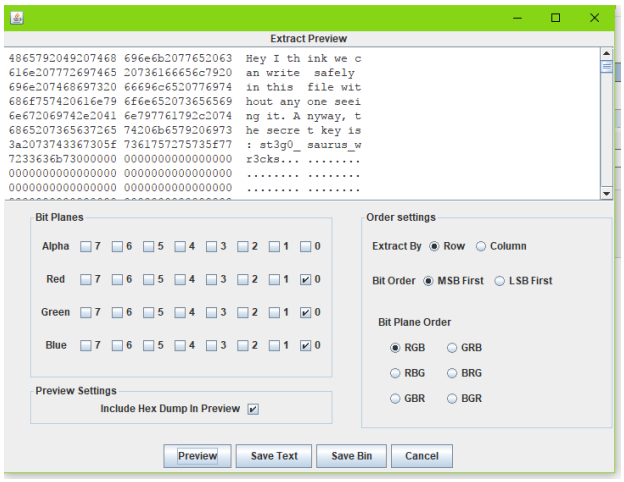
解题链接： http://www.cnblogs.com/Triomphe/p/7586108.html

0x07 *Chromatophoria*

原题链接：http://www.shiyanbar.com/ctf/1988

1.用hex workshop分析，发现有textdata穿件时间，然后用binwalk分析，并没有得到什么关键信息。

2.看题目，他们可能通过颜色的值进行通信，猜测是LSB，用stegsolve分析，在rgb三个颜色的最低位的左上方都有信息。



4.提取，得到key值：**st3g0_saurus_wr3cks**

转载于:https://www.cnblogs.com/Triomphe/p/7635591.html