

# 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>

版权

## 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）

```
0000CB88  C7 FE 00 1F FF D9 50 4B 03 04 14 00 02 00 08 00 F4 02 9F 41 D4 50 D9 9C E3 2D 0123456789ABCDEF0123456789
0000CBA2  00 00 99 2E 00 00 08 00 1C 00 20 20 20 20 20 20 20 20 55 54 09 00 03 8B 4B E1 .....PK.....A.P...-
0000CBB0  50 8C 4B E1 50 75 78 0B 00 01 04 E8 03 00 04 E8 03 00 00 AD 77 F7 37 1B DE .....UT...K.
0000CBD6  1F 77 28 6A 54 6B 6B 29 25 35 A3 A8 AD 94 8F 91 98 0D 42 62 8F D6 2A B1 15 45 P.R.Pux.....w.7..
0000CBF0  8B 52 2A A8 11 7B 8F 58 91 D8 7B 14 B5 B7 D6 88 91 18 B5 DA A2 68 ED 59 4F BF .w(jTkk)%5.....Bb...*..E
0000CC0A  3F 3C 7F C1 F3 BC EE 39 EF 73 CF B9 F7 BC 5F E7 BC D7 7D DD EB B9 EB 6F 00 06 .R*...{.X...{.....h.YO.
0000CC12  1F 77 28 6A 54 6B 6B 29 25 35 A3 A8 AD 94 8F 91 98 0D 42 62 8F D6 2A B1 15 45 ?<.....9.s.....}.....O..
```

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

```
00000000  3F 3F 03 04 0A 00 00 00 00 00 22 79 8E 42 F6 7D 2E EF 1B 00 00 00 1B 00 00 0F 00 1C 00 4D 61 67 37 2D 42 57 2F 6B 2?....."y.B.j.....Mag7-BW/k
00000027  65 79 2E 74 78 74 55 54 09 00 03 D0 FE 6A 51 0B FF 6A 51 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 4B 65 79 3A 20 sy.txtUT.....jQ..jQux.....Key:
0000004E  4E 65 78 74 20 73 74 6F 70 20 54 61 61 75 20 45 72 69 64 61 6E 69 0A 50 4B 03 04 14 00 00 00 08 00 27 B6 47 32 1B A6 C8 Next stop Tau Eridani.PK.....G2...
00000075  9C E4 52 04 00 8C 36 05 00 14 00 1C 00 4D 61 67 37 2D 42 57 2F 43 68 61 72 74 2D 31 35 2E 70 64 66 55 54 09 00 03 BA ..R...6.....Mag7-BW/Chart-15.pdfUT....
```

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

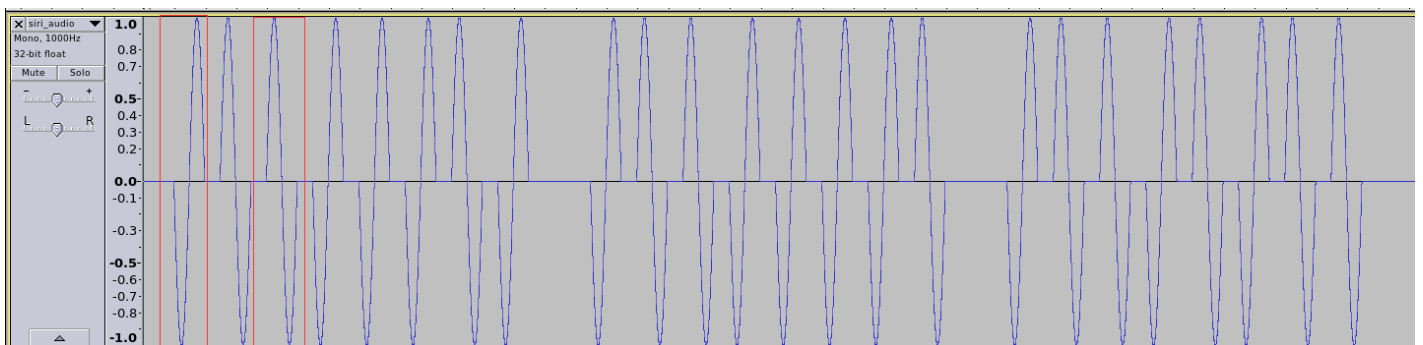
KEY:

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

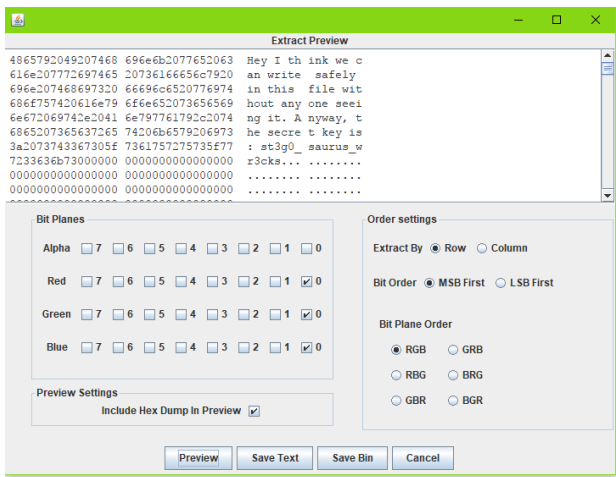
, 原题链接: <http://www.shiyanbar.com/ctf/1989>

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文件时间，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>