ctf隐写术

原创

BetterDream 于 2022-04-25 14:56:30 发布 16 收藏
分类专栏： 隐写术 文章标签： 网络安全

基于文件结构的图片隐写：直接嵌入式隐写，在不影响文件的使用时，在文件中藏入秘密信息，实现信息隐藏；

根据文件特性与冗余性分为：追加插入法和前置插入法，插入信息科分为：文本插入，文件插入；

追加插入法是最常用的，最简单的一种方法，利用文件特性在文件末尾加进行附加数据：

分离文件，一个照片文件里可能有两个照片，组成结构为文件头数据块文件尾文件头数据块文件尾
因为有一个文件尾，所以后一部分的没有被识别出来，使用formost工具分离。

1.PNG图片结构：

标准的PNG文件结构包括：PNG文件标识和PNG数据块。
PNG图片文件结构：

-（固定）8字节89 50 4E 47 0D 0A 1A 0A为png文件头；

-（固定）4字节00 00 00 0D（即十进制的13）代表数据块的长度为13；

-（固定）4字节49 48 44 52（即为ASCII码的IHDR）是文件头数据块的标识（IDCH）；

-（可变）13位数据块（IHDR)

- 前四个字节代表该图片的宽

- 后四个字节代表该图片的高

- 后五个字节依次为：

Bit depth、ColorType、Compression method、Filter method、Interlace method

-（可变）剩余四字节为该png的CRC检验码，由从IDCH到IHDR的十七位字节进行crc计算得到。PNG图片文件头数据块（IHDR）包括：宽、高、图像深度、颜色类型、压缩方法等（图中蓝色的部分即IHDR数据块）。

2.修改高度隐写：

先用TweakPNG打开图片，一般修改过长宽的图片都会报错。

找到PNG图片高度值所对应的位置，并修改为一个较大的值，尝试打开。

修改01 00为02 00，并保存后打开。

修改宽高之后的PNG图片可能打不开，需要修复PNG图片的CRC校验值。

方法：选中PNG的struct IHDR Ihdr部分(图中蓝色部分)，使用CRC Calculator重新计算CRC校验值。

将struct IHDR Ihdr的CRC（图中蓝色部分）修改为重新计算过的CRC。

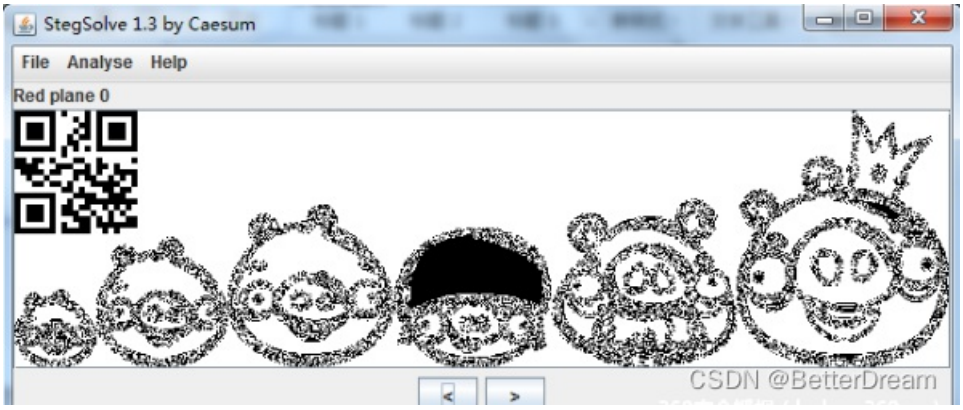
再用TweakPNG打开图片不报错，修复成功。

3.IDAT块的隐写：

PNGCheck可以验证PNG图片的完整性（通过检查内部CRC-32校验和&bra;比特&ket;)和解压缩图像数据，它能够转储几乎所有任选的块级别信息在该图像中的可读数据。查询命令：pngcheck -v xxx.png

基于LSB原理的图片隐写：

1. 简单的LSB隐写：替换隐藏（lsb）
图片中的像素是三种颜色组成的，png中每个颜色有8bit，lib隐写是修改了像数中的最低的1bit
在肉眼中看不出来，也就把信息隐藏了起来，颜色可能变淡，肉眼看不出来区别
分析LSB隐写，使用stegsolve工具。藏有二维码，使用QR Reserach。利用LSB（最低有效位 (Least Significant Bit)来进行隐写。例如在PNG图片的储存中，每个颜色会有8bit，LSB隐写就是修改了像数中的最低的1bit，人眼无法区别。例如我们想把A隐藏进来的话，可以把A转成16进制的0x61再转成二进制的01100001，再修改为红色通道的最低位为这些二进制串。分离方法：Stegsolve分离：使用Stegsolve—Analyse—Frame Browser，可以浏览三个颜色通道中的每一位。



PS：此种隐写的载体一般为png或bmp格式，jpg的有损压缩方式会破坏隐写的内容。

图片容差隐写：

1.背景知识：

容差，在选取颜色时所设置的选取范围，容差越大，选取的范围也越大，其数值是在0-255之间。

2.容差比较的隐写：

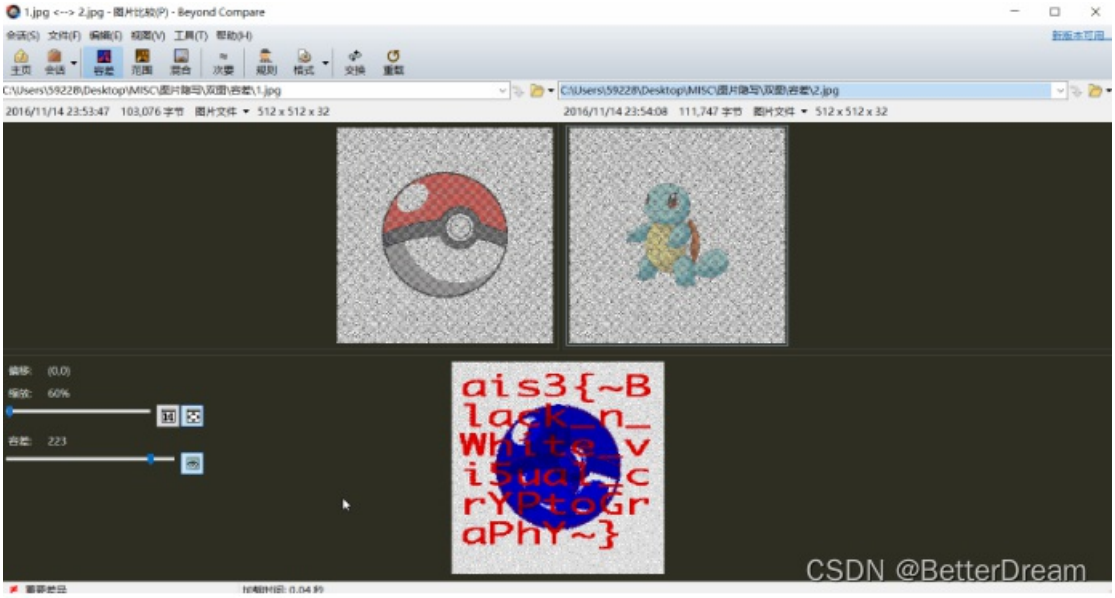
分离方法：

beyond compare分离：

操作步骤：

打开工具，选择图片比较，导入example_1.jpg和example_2.jpg。

选择容差模式，并调整容差大小



PS：

Beyond Compare4|Beyond Compare破解版激活码：

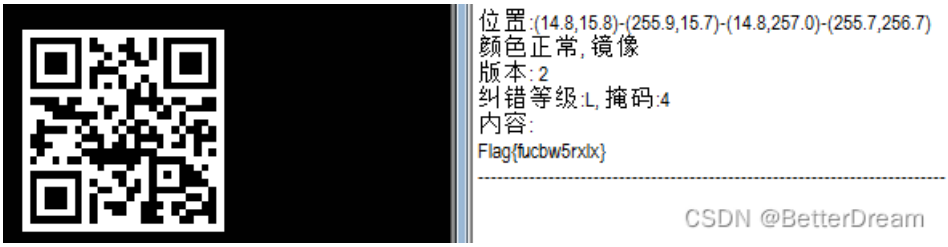
1、L2aJTd2SauPv4Luhang21uqq5NJOEw94wxdZTpU-pFB9GmyPk677gJ

2、RuGuo7nimugASTzh99xsaioxTsE2-oigiuomj+JHFjazxsaoh43kmplmjx

3、hFbqTmYskatMTgPyjvv99CF2Te8ec+Ys6PPxyZAF0YwOGUlLOO98iug

二维码隐写：

使用QR Research读取二维码中的信息。



常用文件头尾标识：

常见图片文件头尾标识：
JPEG/JPG：
文件头标识(2 bytes)：FF D8
文件结束标识(2 bytes)：FF D9
PNG：
文件头标识(8 bytes)：89 50 4E 47 0D 0A 1A 0A
GIF：

文件头标识(6 bytes)：47 49 46 38 39(37) 61
文件结束标识(2 bytes)：01 01 00 3B
BMP：
文件头标识(2 bytes)：42 4D