CTF常用隐写套路

转载

小毛毛2013 于 2018-08-24 13:34:23 发布 14130 收藏 42
分类专栏： 安全


安全 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

隐写术是一门关于信息隐藏的技巧与科学，所谓信息隐藏指的是不让除预期的接收者之外的任何人知晓信息的传递事件或者信息的内容。隐写术的英文叫做Steganography，来源于特里特米乌斯的一本讲述密码学与隐写术的著作Steganographia，该书书名源于希腊语，意为“隐秘书写”。

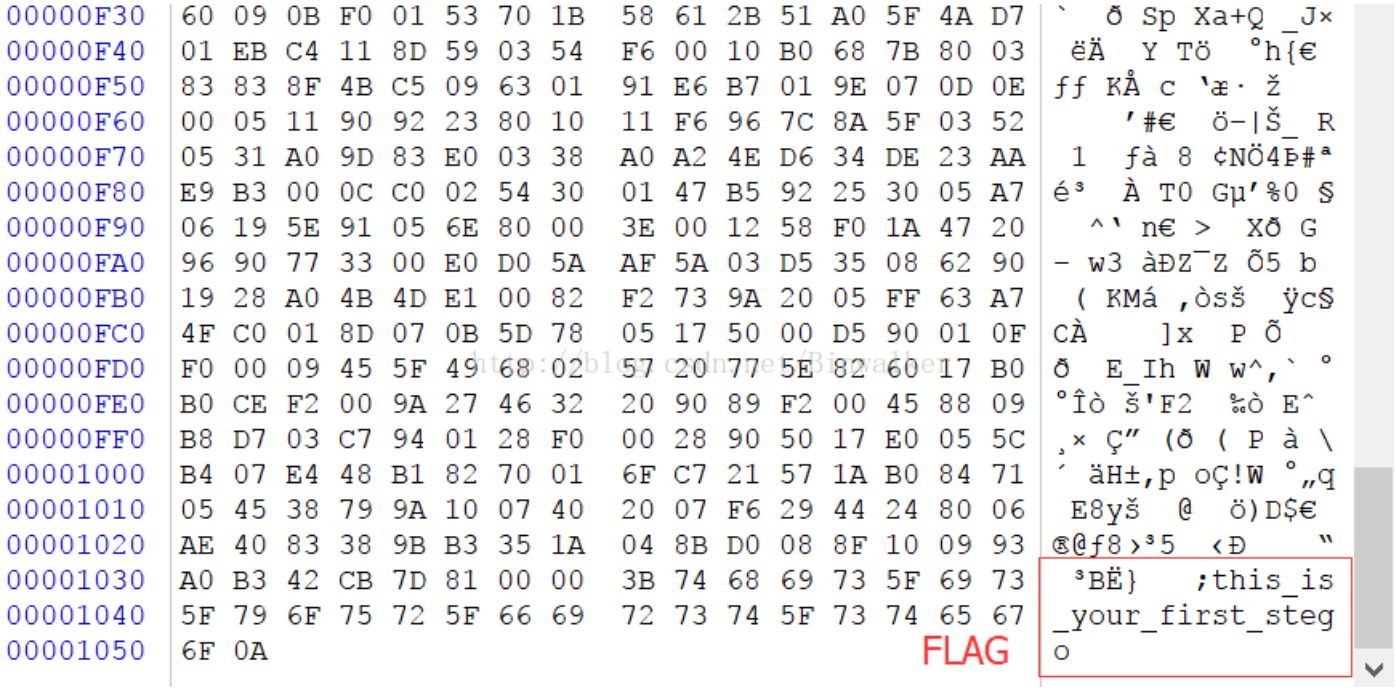
在CTF题目中，图片隐写题属于杂项的一部分，题目较为简单。本文大致梳理了下CTF比赛中图片隐写题的常用套路，如果未能看出题目破题点，可按照以下方法顺序逐一尝试：

1. 查看图片基本信息（对应题目难度：低）

该类题通过查看图片基本信息，可以直接获取FLAG，主要方法如下：

A）右键查看图片属性，检查图片简介、备注中是否有FLAG；

B）将图片用编辑器工具打开，如使用记事本、notepad+、winhex，检查是否包含FLAG；

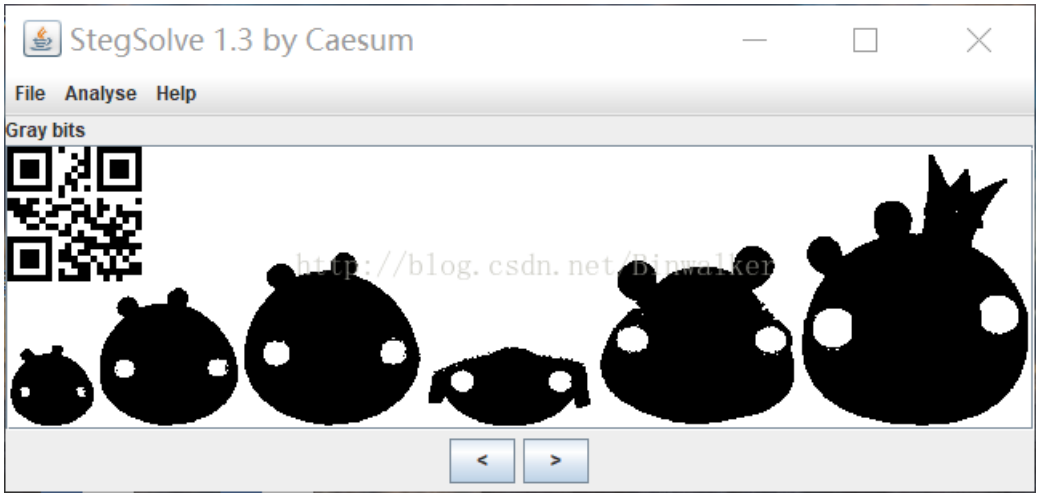


2. 多图层文件（对应题目难度：中）

玩CTF的大概都听过一个神器 - stegsolve，用它把图片打开，该软件也有两种用途：

A）一直按右箭头（或者左箭头），说不定就会出来一个二维码；

B）提取低位信息，这涉及到图片隐写的一个大类，lsb隐写，一般都藏在0,1,2这些低位里面，在软件功能选项中查看Analyse→Data Extract，逐个调试。



3. 复合文件（对应题目难度：中）

CTF比赛中经常碰到png文件中复合其他文件的情况，如就是图片后面再放点压缩包、txt文档、或者再添加一张图片，具体操作方法如下：

copy /b a.jpg+b.zip c.jpg

copy /b a.jpg+b.txt c.jpg

copy /b a.jpg+b.jpg c.jpg

解题思路：通常这类图片比较大，可将图片后缀改为zip或者rar，解压即可。也可以用winhex找图片的开头结尾标志，手动分离出来，也可以使用kali下的工具binwalk或者foremost分出来；

注：比较高级点的图片隐藏图片的话，有的会把第二张图片头给去掉，然后把两张图片合在一起，这样那些提取工具就没用了，这个时候需要稍微细心点，用winhex找第一张图片的尾部，然后把第二张图片的头给加一下，再进行分离操作。

4. 改图片高度（对应题目难度：中）

CTF比赛中可利用16进制编辑工具更改图片的高度，使图片只显示一部分，下面的部分被隐藏，嗯，这是个藏东西的好办法！

当以上方法均不可以得到FLAG，且图片长宽比例诡异时，可以尝试改图片大小，下面介绍找图片宽度和高度的标志位的方法：

A）对于png文件，其第二行第六列是高度位，改这一位即可；

B）对于其他格式图片，可以先看看图片的属性，得到宽高值，转成16进制数，搜索该16进制值就能找到标志位了；

本文仅列举了几种博主目前遇到的CTF图片隐写套路，欢迎大家补充!