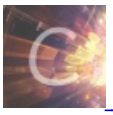
stegsolve图片隐写解析器的使用

原创

黑朱雀 于 2021-02-19 09:29:07 发布 2242 收藏 17

分类专栏： 网络安全

本文链接：https://blog.csdn.net/weixin_43639682/article/details/113857310



---

layout: post

title: “ctf-隐写图片解析器-stegsolve的使用”

categories: [ctf]

tags: [stegsolve]

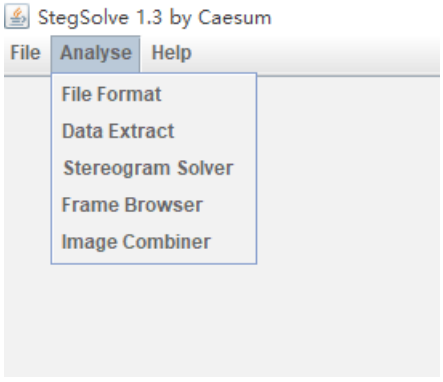
CTF隐写术————隐写图片解析神器----**stegsolve**

stegsolve下载地址：http://www.caesum.com/handbook/Stegsolve.jar

stegsolve安装配置：配置好Java环境变量（就是需要安装Java，然后配环境变量，具体的配置过程上网一搜一堆，这里就不赘述）

配置好环境之后直接打开就可以使用

文件打开保存退出，没什么好说的



在分析里面从上到下的依次意思是

File Format:文件格式

Data Extract:数据提取

Steregram Solve:立体试图 可以左右控制偏移

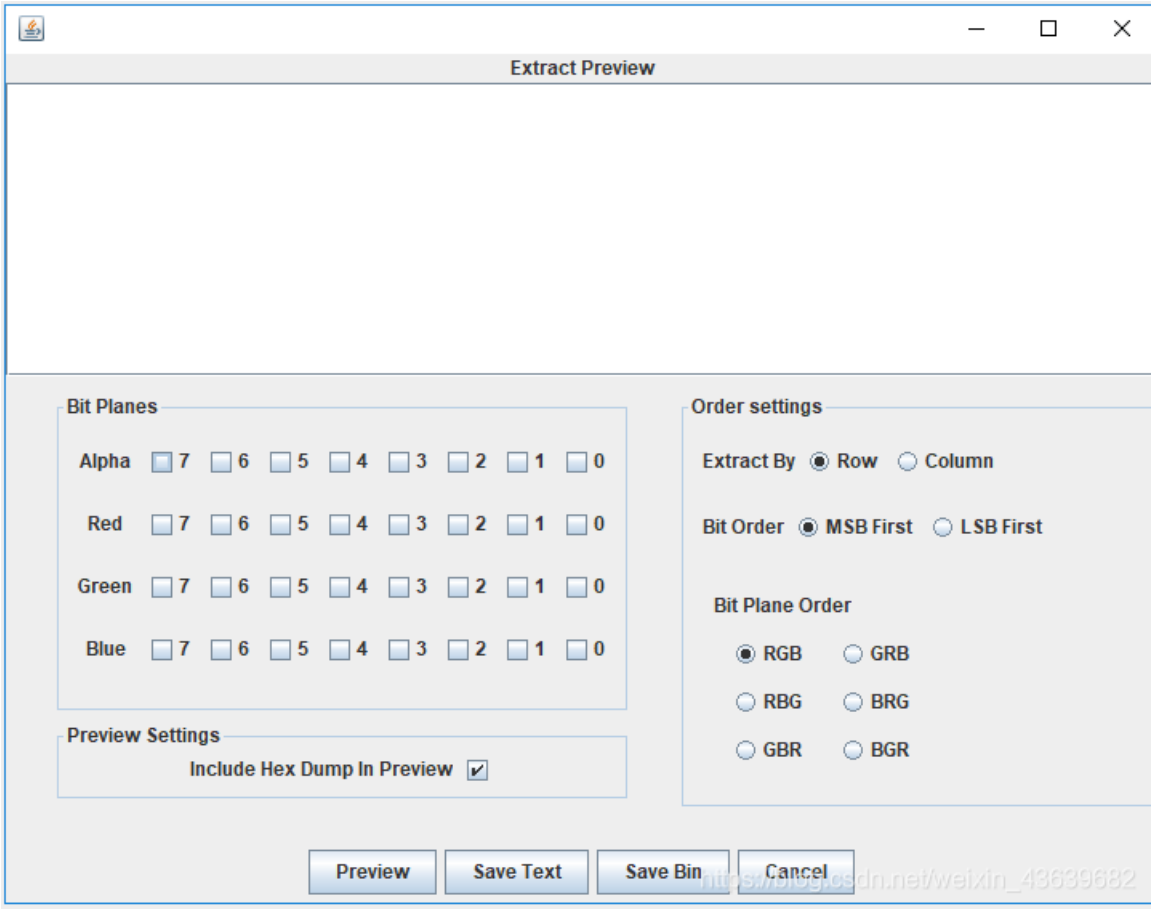
Frame Browser:帧浏览器

Image Combiner:拼图，图片拼接

用法（使用场景）

1.File Format:这里你会看见图片的具体信息有时候有些图片隐写的flag会藏在这里

2.Data Extract:(好多涉及到数据提取的时候，很多博主在wp中都是一带而过，小白们还以为要一个个试。。)



左边一大部分主要是讲了RGBA（Alpha是透明度）的颜色通道

为了方便理解我们分开说

RGB是红绿蓝 但他们的值代表的实际上是亮度

R的数字越大，则代表红色亮度越高；R的数字越小，则代表红色亮度越低。G，B同理

R的亮度各有256个级别，GB同理。即从0到255，合计为256个。从数字0到255的逐渐增高，我们人眼观察到的就是亮度越来越大，红色、绿色或蓝色越来越亮。然而256是2的8次方 所以你会看见上图的7~0 一共8个通道

而Alpha就是透明度 该通道用256级灰度来记录图像中的透明度信息，定义透明、不透明和半透明区域

alpha的值为0就是全透明，alpha 的值为 255 则表示不透明

因此左半部分就理解了

右半部分就是Extra By(额外的)和Bit Order（位顺序）和Bit Plane Order（位平面的顺序）

1）.Extra By(额外的)：分为row（行）和column（纵）

每个像素用R，G，B三个分量表示，那么一张图片就像一个矩阵，矩阵的每个单位就是（0_{255}, $_0255$，0~255）

也就会有是纵排列和行排列了，一般事先访问行再访问列（如果相反会引起ve使用方法）

2）.Bit Order（位顺序）:MSB是一串数据的最高位，LSB是一串数据的最低位。

3）.Bit Plane Order（位平面的顺序)

整个图像分解为8个位平面，从LSB(最低有效位0)到MSB（最高有效位7）随着从位平面0 到位平面7，位平面图像的特征逐渐变得复杂，细节不断增加。（一般我们的图片如果是RGB那么就是24位 3乘8嘛）

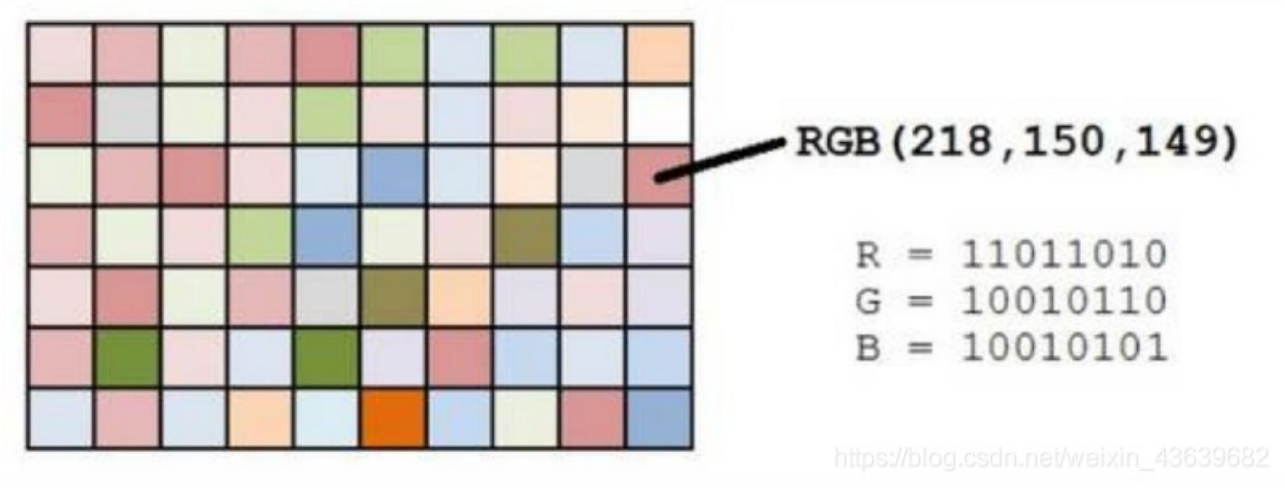
4）Bit Plane Order（位平面的顺序）:一般图片是24位 也就是3个8 大家可以想像成三明治 比如BGR就是B为三明治第一层 G为第二层 R为第三层。

3.Steregram Solve:立体试图 可以左右控制偏移 可以放张图片试一下就知道这个是什么意思了

4.Frame Browser:帧浏览器 主要是对GIF之类的动图进行分解，把动图一帧帧的放，有时候会是二维码

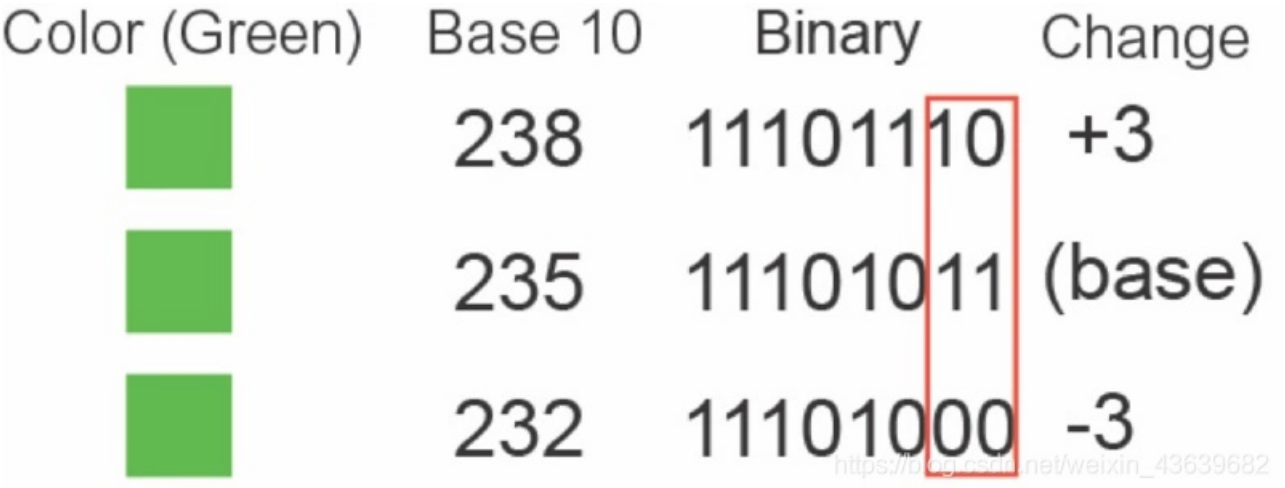
5.Image Combiner:拼图，图片拼接（意思显而易见）

接下来会带大家实战去深入理解一下Data Extract里面ctf经常用到的LSB隐写

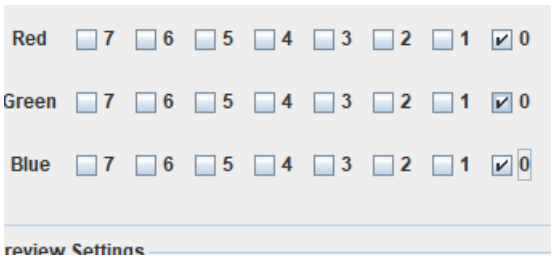


这个我们之前介绍的很详细

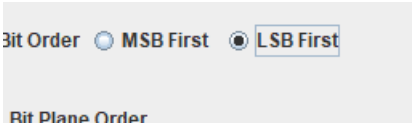
而LSB隐写就是修改RGB颜色分量的最低二进制位也就是最低有效位（LSB），而人类的眼睛不会注意到这前后的变化，（人类的眼睛只能识别一部分颜色的变化）



如果我们修改lsb那么颜色依然和没修改的一样，并且修改的话每个像数可以携带3比特的信息。



这个作用是在于把最低位的二进制全部提取出来



这个作用在于对提取出来的最低位使用lsb解码算法