

# CTF-隐写术（十一）

原创

红烧兔纸 于 2020-09-26 22:23:28 发布 307 收藏 4

分类专栏: [CTF-隐写术](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_39934520/article/details/108818107](https://blog.csdn.net/weixin_39934520/article/details/108818107)

版权



[CTF-隐写术 专栏收录该内容](#)

14 篇文章 2 订阅

订阅专栏

声明: 以下CTF题均来自网上收集, 在这里主要是给新手们涨涨见识, 仅供参考而已。需要题目数据包的请私信或在下方留言。

## 21.SB! SB! SB! (来源: 实验吧)

### 1.关卡描述

SB! SB! SB! 分值: 20

来源: 西普学院

难度: 中

参与人数: 7499人

Get Flag: 3243人

答题人数: 3317人

解题通过率: 98%

LSB

解题链接: <http://ctf5.shiyanbar.com/stega/ste.png>

[https://blog.csdn.net/weixin\\_39934520](https://blog.csdn.net/weixin_39934520)

### 2.解题步骤

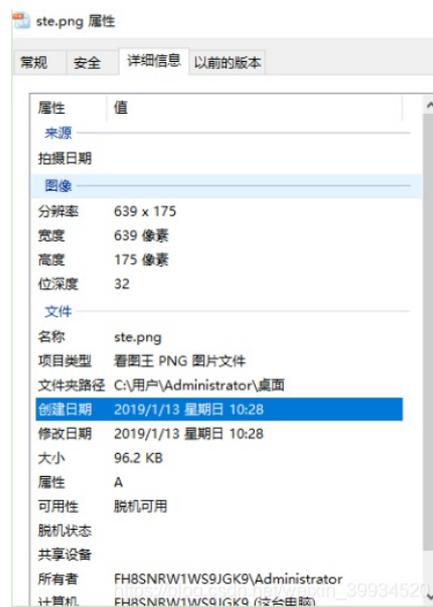
分析:

这种信息隐藏的方式使用了LSB算法,因此题目名称为:SB! SB! SB!也相当于是给了我们一点提示吧。)

下载题目提供的图片



发现是png格式,打开属性看看



并没有发现有用的信息,看到图片名称为:ste.png,提示我们这道题属于图片的隐写使用UE打开图片查看文件的16进制编码

也没有在文件的头部和尾部发现特殊信息

现在考虑到隐写信息可能就是在图片的内容中,用Windows自带图片浏览器打开发现是疯狂的小鸟中的游戏元素

也没有发现异常,这时,想到使用Stegsolve.jar来查看图片的通道信息(注:一般如果发现是png格式的图片,则考虑使用上述工具查看通道信息,成功几率非常大)

打开后,我们一次查看所有通道.



在red plane0通道中,发现一个二维码.  
截图保存:



利用QR解码:

或者网站 <http://jiema.wwei.cn/>



**flag{AppLeU0}**

22.当眼花的时候,会显示两张图(来源:实验吧)

1.关卡描述

当眼花的时候，会显示两张图 分值：30

来源：西普学院

难度：难

参与人数：5594人

Get Flag：560人

答题人数：621人

解题通过率：90%

不信？你试试

解题链接：<http://ctf5.shiyanbar.com/stega/final.png>

[https://blog.csdn.net/weixin\\_39934520](https://blog.csdn.net/weixin_39934520)

## 2. 解题步骤

分析：

下载图片：



题目已经提示有两张图片

那就把第二张图片找出来

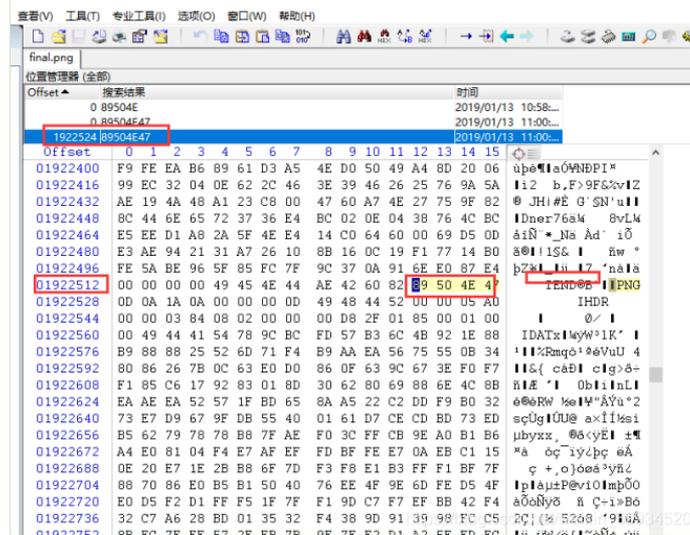
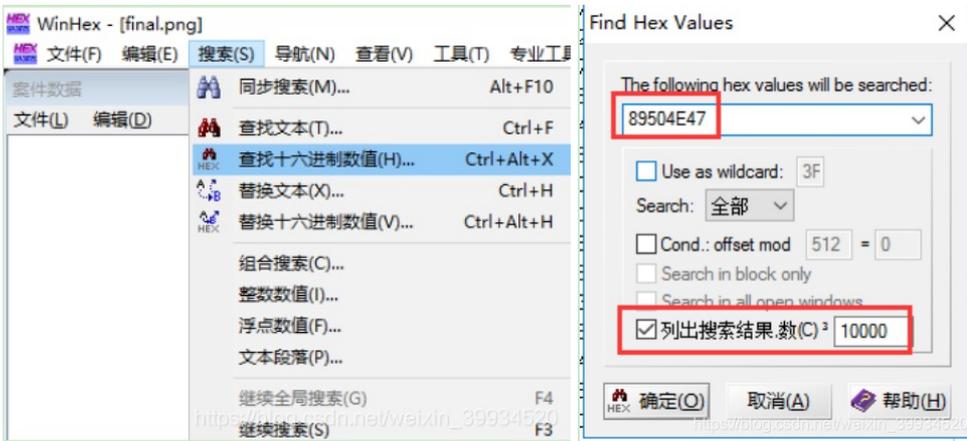
一般使用工具：**binwalk** 查看是否隐藏其它文件，再利用**-e** 或**-cp**命令或者**foremost**分离。不过我电脑暂时没有装这两个工具。

使用**winhex**

已知PNG格式的图片的文件头为：**89504E47**

在**winhex**打开**final.png**

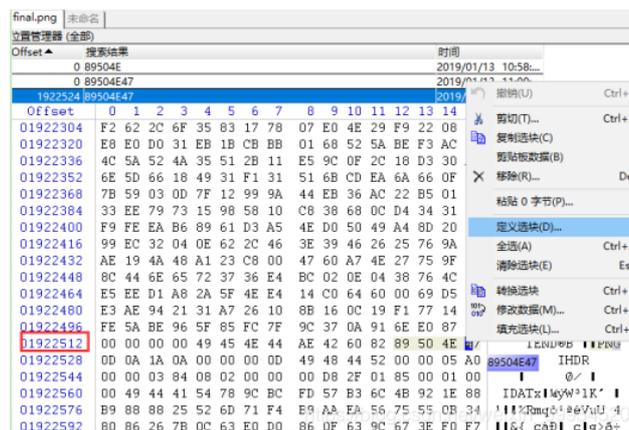
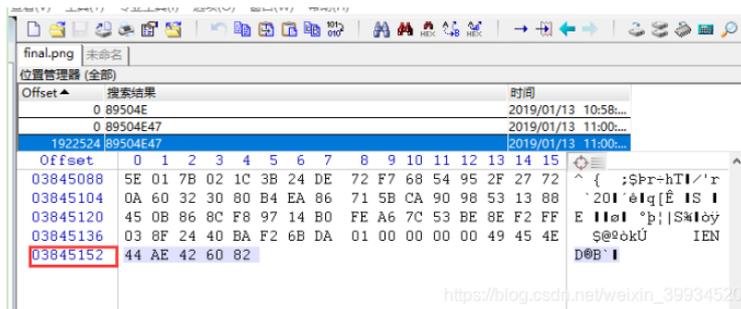
搜索关键词：**89504E47**



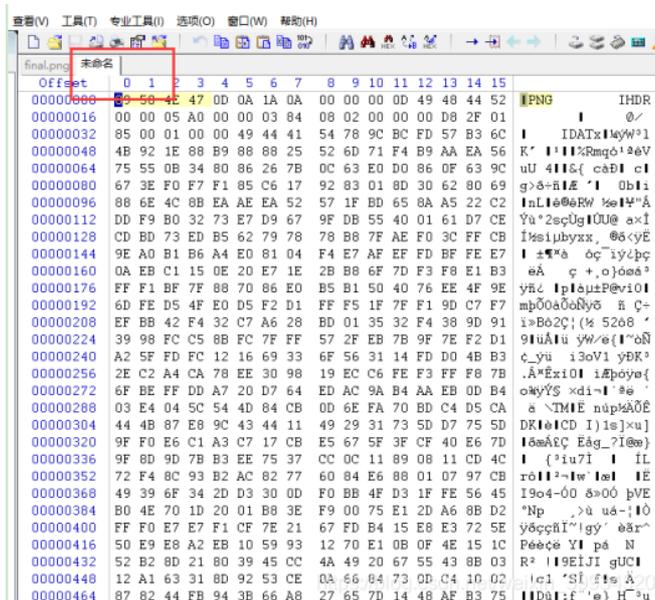
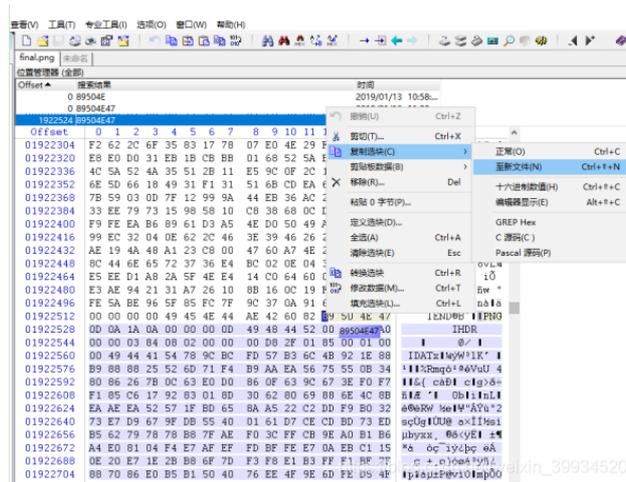
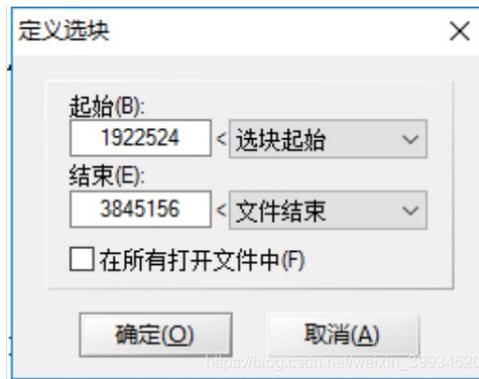
发现另一个.png格式的图片

分离另存为1234.png图片

分离图片的方法:



注意定义选块很重要:



另存为为1234.png

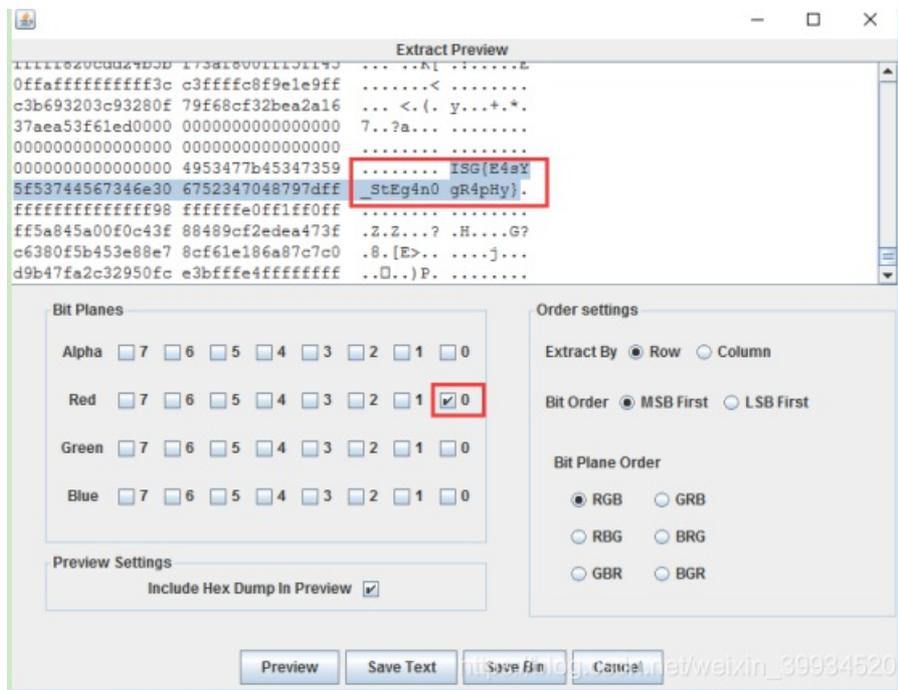
打开发现和原来图片一样。不过还是可以发现一些16进制字符有所不同

利用神器stegsolve, 打开1234.png, 利用通道逐个查看, 并未什么发现

再继续使用data extract

最低位可以一个一个的去试一试:

勾选red(0)



ISG{E4sY\_StEg4n0\_gR4pHy}