

# A\_Writeup\_杂项“百越杯”第四届福建省高校网络空间安全大赛——致我的战队HeroCat的所有成员...

转载

[weixin\\_30346033](#) 于 2018-12-01 21:33:00 发布 108 收藏  
原文链接: <http://www.cnblogs.com/HeroCat/p/10051115.html>  
版权

0x00 题目名称

签到

操作内容:

1、搜索:

The screenshot shows a Baidu search result for '在线数独解题'. The search bar contains the text '在线数独解题'. Below the search bar, there are navigation tabs for '网页', '资讯', '贴吧', '知道', '视频', '音乐', '图片', '地图', and '文库'. The search results show approximately 606,000 results. The top result is '琳琅在线-数独求解器', with a description: '数独题库,数独游戏题目,数独技巧,数独求助,数独求解器,数独排行榜,数独计算器... 琳琅在益智游戏 >> 数独游戏 >> 数独求解器 数独游戏数独题库 数独知识...'. Below the search results, there are recommendations for '数独在线解答器', '数独答案生成器网页', '6宫格数独在线解题器', '数独破解软件', '数独快速解法', '1——9九宫格数独口诀', and '六字数独解法'.

2、将内容填入

The screenshot shows a Sudoku solver interface with three buttons: '导入', '重置', and '开始求解'. The '开始求解' button is highlighted with a red box.

4	7	3	6	1	5	9	2	8
2	1	6	9	8	4	7	5	3
5	9	8	2	3	7	1	6	4
6	5	1	8	9	2	4	3	7
9	4	2	3	7	6	8	1	5
3	8	7	4	5	1	2	9	6

8	3	4	5	2	9	6	7	1
1	2	5	7	6	8	3	4	9
7	6	9	1	4	3	5	8	2
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>

FLAG 值:

FLAG{cee3860fb3f4a52e615fa8aaf3c91f2b}

0x01 题目名称 **马男波杰克**

操作内容:

1、搜索: atool, 在网站的搜索栏搜索隐写术



上传图片



2. 输入需要解开信息的密码 (如果没有密码可以不填) : 信息查看密码, 可以为空即为图片解密不需要密码

解密出隐藏的信息

## 二、解密带隐藏信息的图片

1. 从电脑中选择一张带有隐藏信息的图片: 选择文件 atool.png

2. 输入需要解开信息的密码 (如果没有密码可以不填) : 信息查看密码, 可以为空即为图片解密不需要密码

解密出隐藏的信息

图片中隐藏的信息为: flag{jioiuojoi666}

flag

说明 | Introduce

1. 隐写术算是一种加密技术, 权威的wiki说法是“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他人

FLAG 值:

flag{jioiuojoi666}

0x02 题目名称: 血小板天下第一可爱

操作:



1.png



key.png

1、先对缺损的二维码进行处理:  
用画图工具将缺损的地方补全



2、对二维码进行扫码：

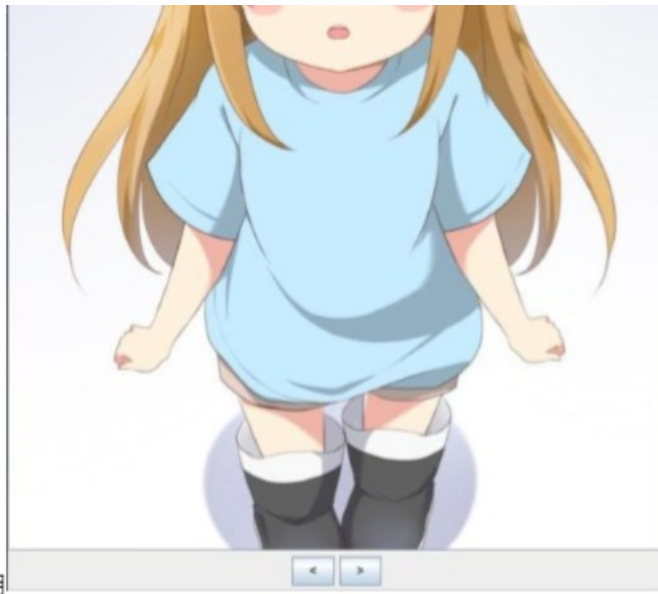


在进行 base64 解密：key%3A%20Lsb\_1s\_gr3at ，

%3A%20 是 Unicode 的冒号：

所以：key: Lsb\_1s\_gr3at



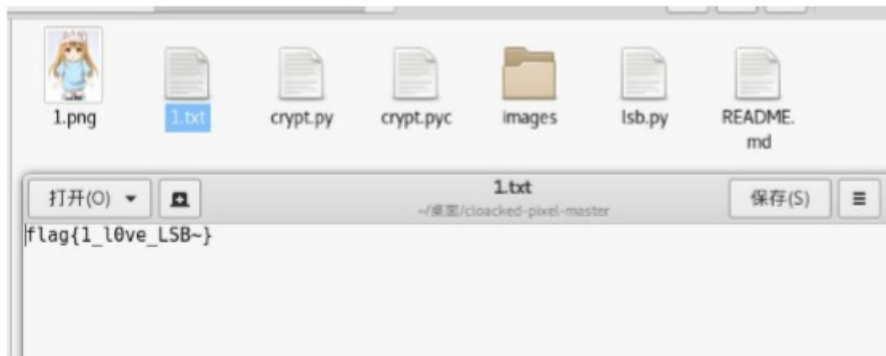


采用 进行处理  
发现无法得出 flag  
所以，只好用自己找来的 py 脚本进行破解

```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@kali: ~/桌面/cloacked-pixel-master# python lsb.py extract 1.png 1.txt Lsb_1s
_gr3at

[+] Image size: 640x841 pixels.
[+] Witten extracted data to 1.txt.
root@kali: ~/桌面/cloacked-pixel-master#
root@kali: ~/桌面/cloacked-pixel-master#
root@kali: ~/桌面/cloacked-pixel-master#
```

将 1.png 解密的结果存到 1.txt 当中，并用上 Lsb\_1s\_gr3at 作为密码



flag{1\_10ve\_LSB~}

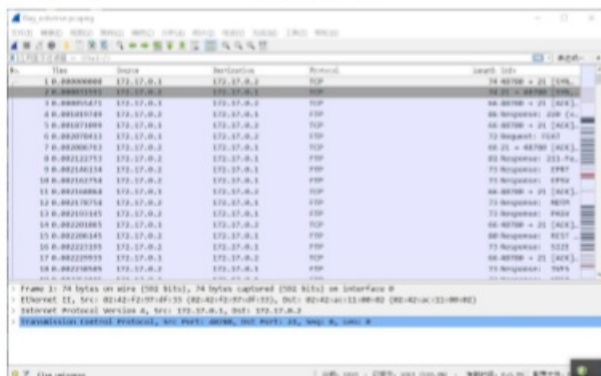
### 0x03 题目: flag\_universe

#### 操作:

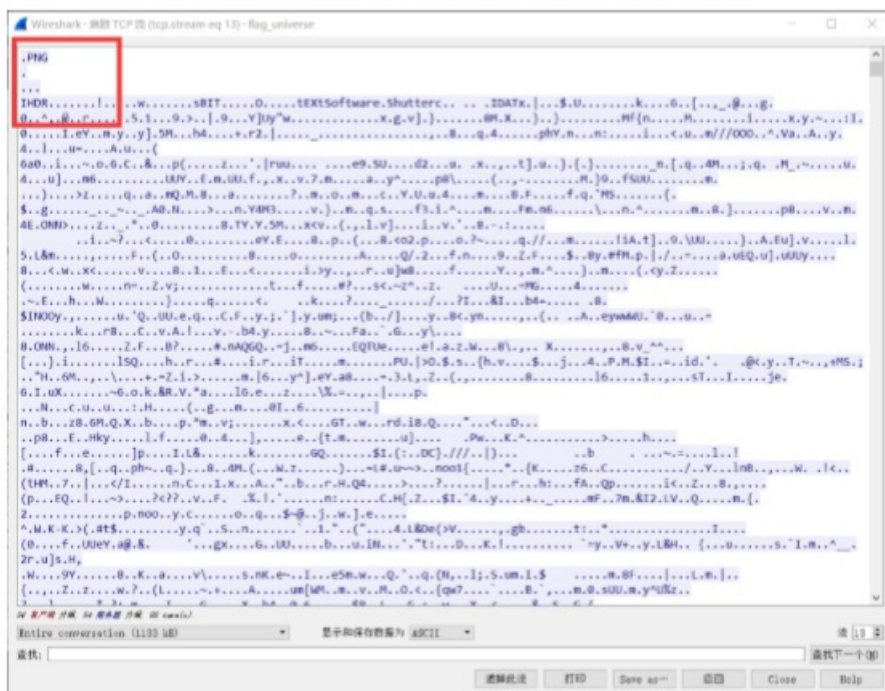




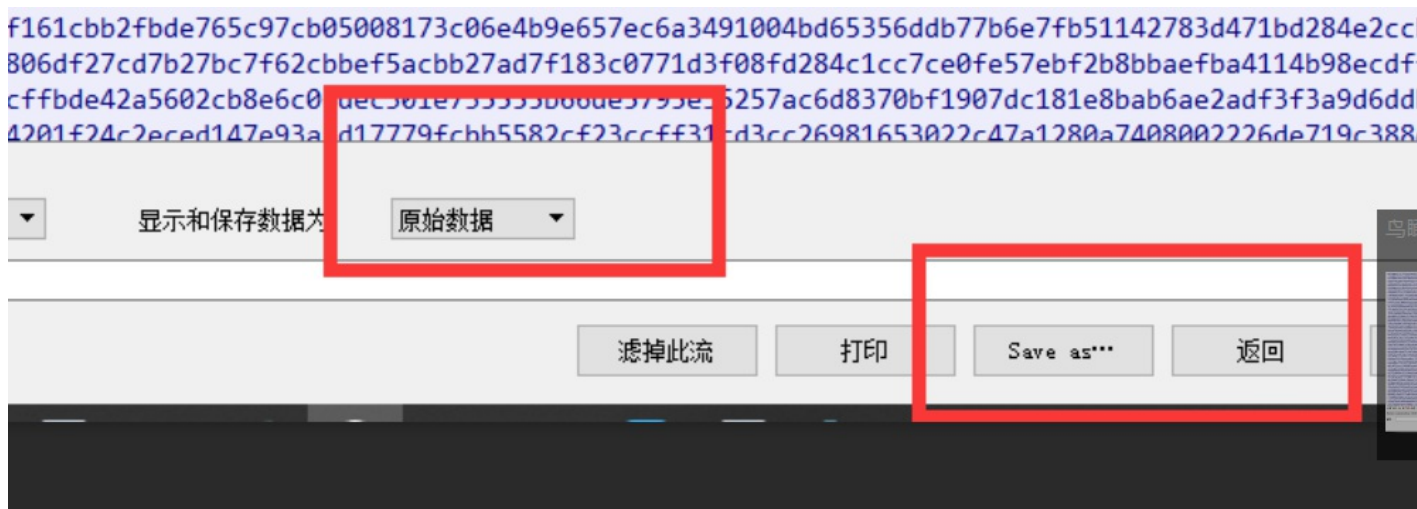
- 1、很显然这是一个抓取的数据包
- 2、采用 wireshark 进行数据分析



因为协议类型基本都为 tcp，所以右键追踪 tcp 流，在 tcp.stream eq 13 以及 tcp.stream eq 14 会发现很长的一大串数据，这是比较突出的，所以，很有可能有 flag 的信息

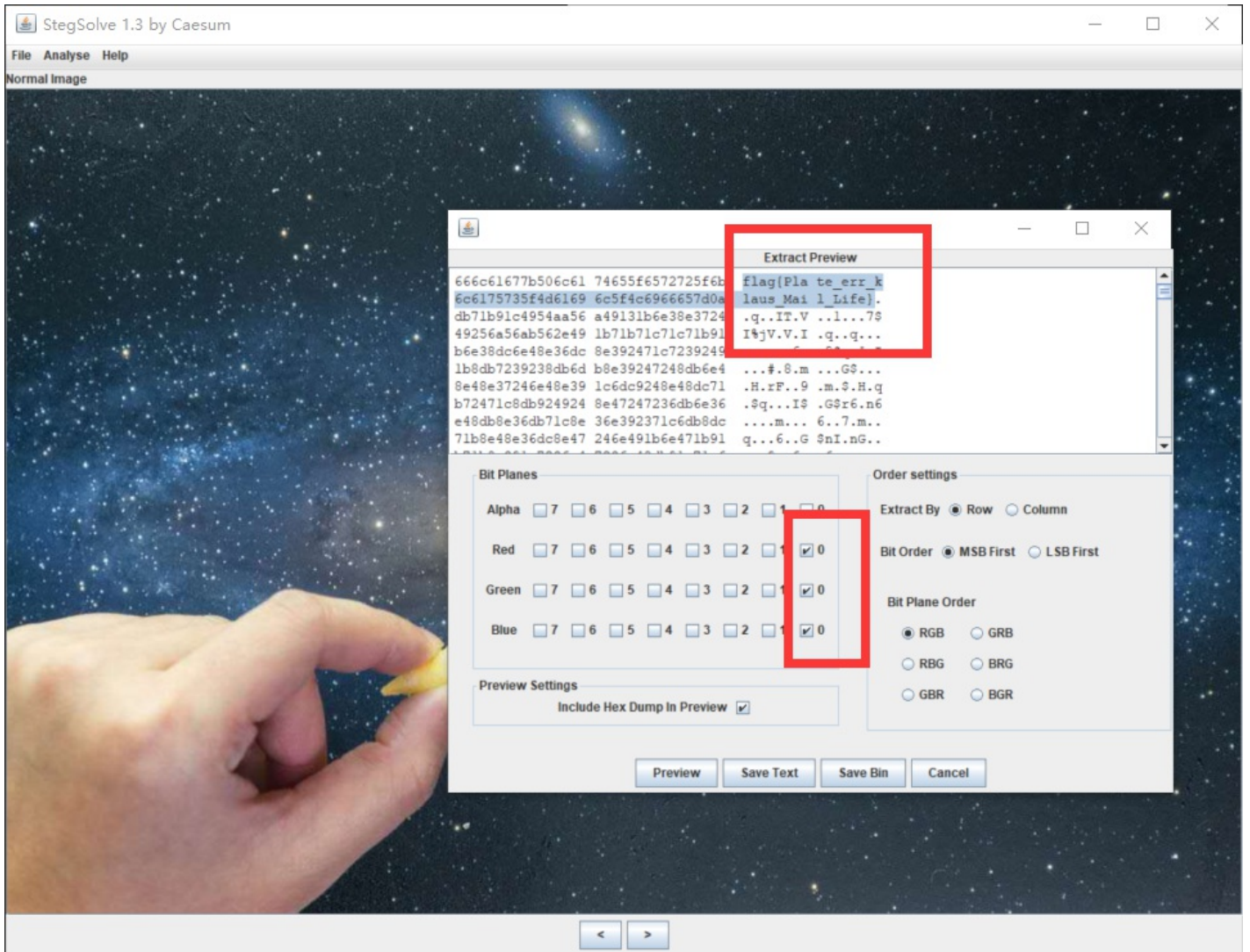
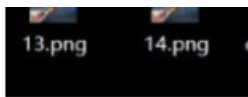


**极有可能是图片**



以相同的方式将 tcp.stream eq 13 以及 tcp.stream eq 14 保存为图片 13.png 和 14.png





**flag{Plate\_err\_klaus\_Mail\_Life}**

作者: HeroCat

出处: <https://www.cnblogs.com/HeroCat/>

特此声明: 欢迎园子的大大们指正错误, 共同进步。如有问题或建议, 也请各位大佬多多赐教! 如果您觉得文章对您有帮助, 可以点击文章右下角【推荐】一下。

版权声明: 本文版权归作者和博客园共有, 欢迎转载, 但未经作者同意必须保留此段声明, 且在文章页面明显位置给出原文链接。

转载于: <https://www.cnblogs.com/HeroCat/p/10051115.html>