xctf攻防世界 MISC高手进阶区 misc_pic_again

原创

l8947943 于 2022-01-14 18:11:08 发布 5652 收藏

分类专栏： 攻防世界misc之路 文章标签： misc

本文链接：https://blog.csdn.net/l8947943/article/details/122499487

攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

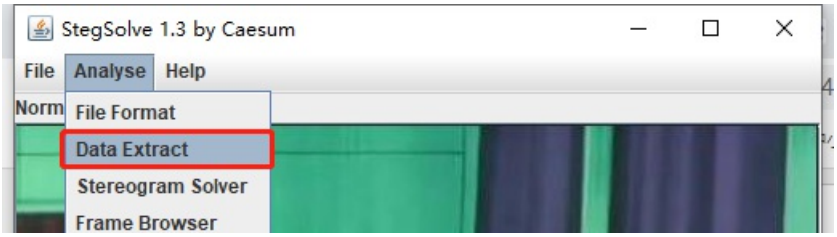
1. 进入环境，下载附件

一张png图片，如图：

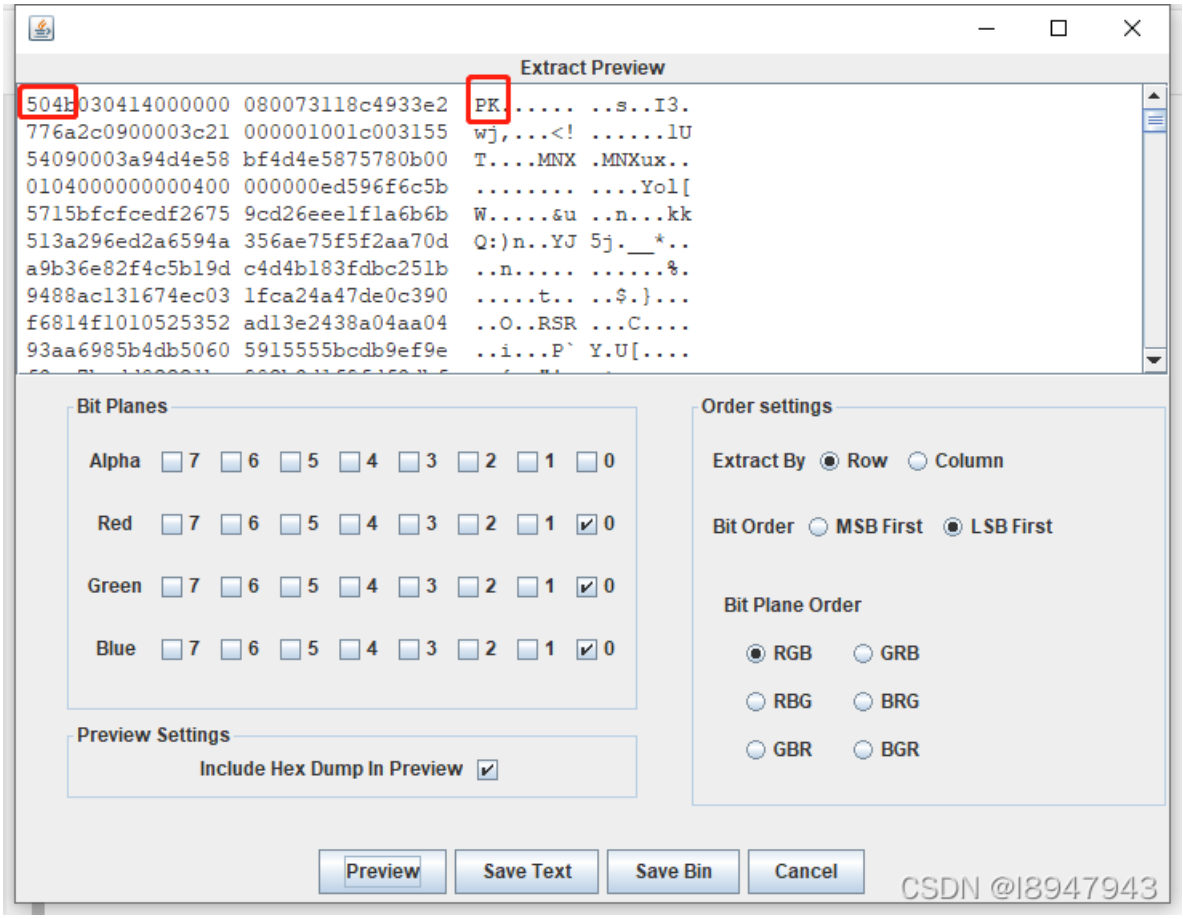
没有其他提示

2. 问题分析

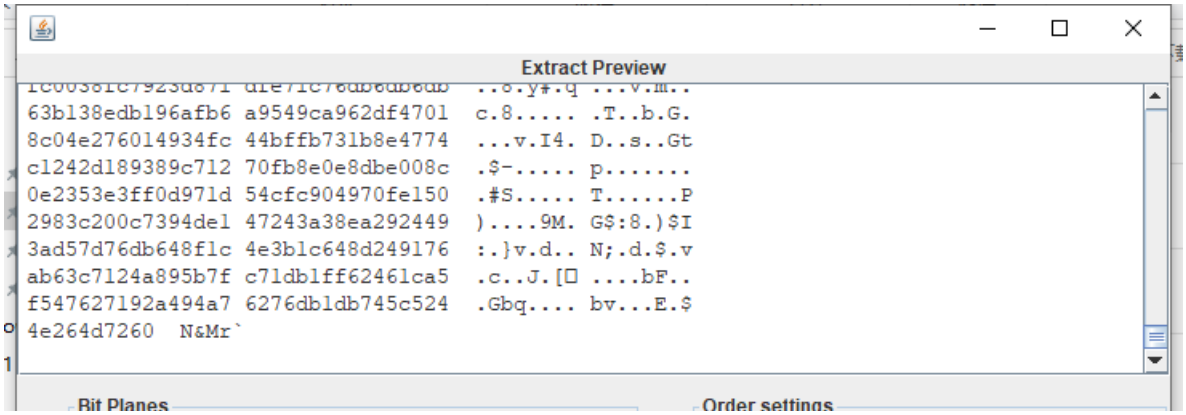
1. **winhex大法**
   一通操作无果
2. **binwalk大法**
   一通操作无果
3. **StegSolve大法**
   这点我属实没思路，参考大佬wp：

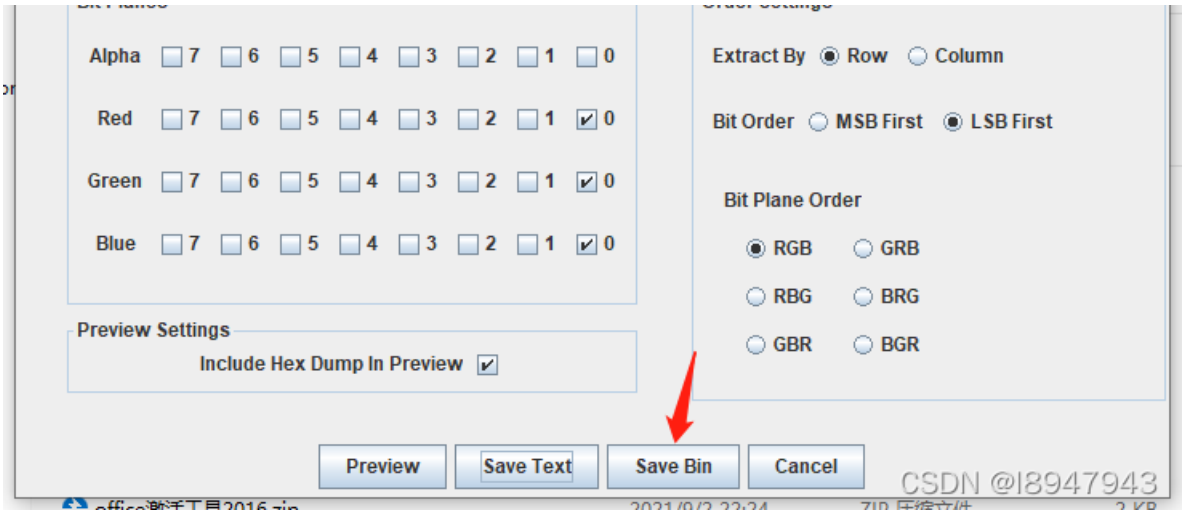


在BitPlanes界面，提取RGB为0通道的，点击Preview，发现提取的内容，开头以PK开始，如图：

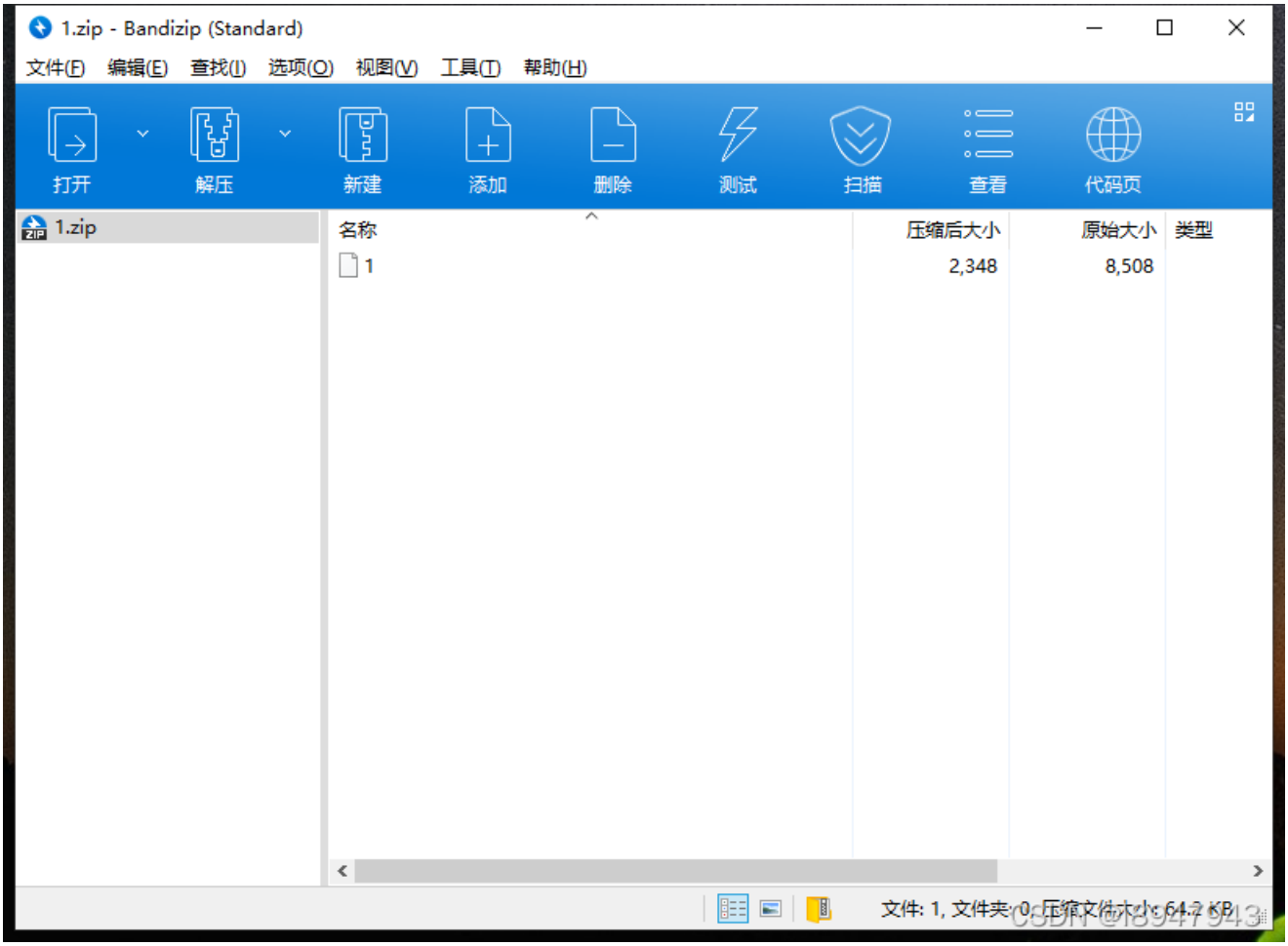


也就是说，提取的这个文件是.zip隐写的内容（如何判断，参考之前的文件标识推断：**https://blog.csdn.net/holandstone/article/details/7624343**），我们将其保存为.zip文件

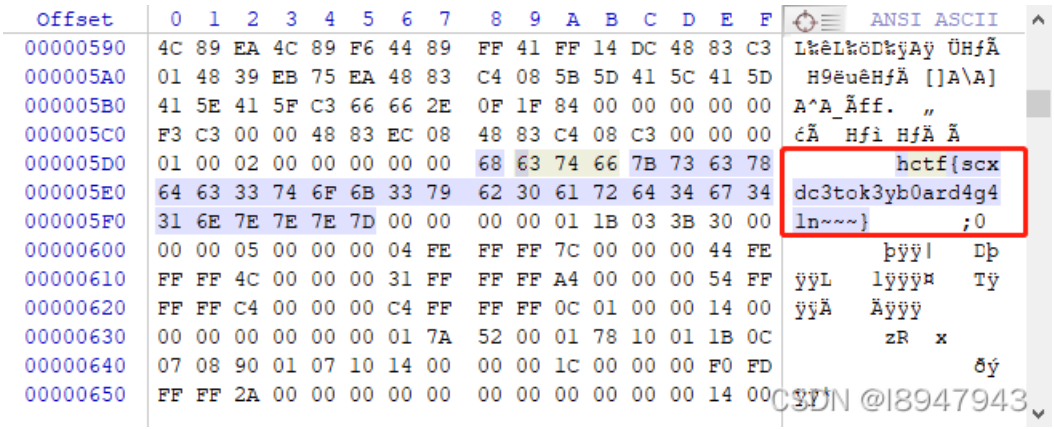



Alpha 7 6 5 4 3 2 1 0
Red 7 6 5 4 3 2 1 0
Green 7 6 5 4 3 2 1 0
Blue 7 6 5 4 3 2 1 0
Extract By Row Column
Bit Order MSB First LSB First
Bit Plane Order
RGB GRB
RBG BRG
GBR BGR
Preview Settings
Include Hex Dump In Preview
Preview
Save Text
Save Bin
Cancel
CSDN @l8947943

打开，如图：


1.zip - Bandizip (Standard)
文件(F) 编辑(E) 查找(I) 选项(O) 视图(V) 工具(T) 帮助(H)
打开
解压
新建
添加
删除
测试
扫描
查看
代码页
1.zip
名称
压缩后大小
原始大小
类型
1
2,348
8,508
文件: 1, 文件夹: 0, 压缩文件大小: 64.2 KB
CSDN @l8947943

将压缩文件里的内容丢入winhex，在文本中搜flag或者ctf，如图：



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000590	4C	89	EA	4C	89	F6	44	89	FF	41	FF	14	DC	48	83	C3	L‰êL‰öD‰ÿAÿ ÜHƒÃ
000005A0	01	48	39	EB	75	EA	48	83	C4	08	5B	5D	41	5C	41	5D	H9ëuêHƒÄ []A\A]
000005B0	41	5E	41	5F	C3	66	66	2E	0F	1F	84	00	00	00	00	00	A^A_Ãff. „
000005C0	F3	C3	00	00	48	83	EC	08	48	83	C4	08	C3	00	00	00	óÃ Hƒì HƒÄ Ã
000005D0	01	00	02	00	00	00	00	00	68	63	74	66	7B	73	63	78	hctf{scx
000005E0	64	63	33	74	6F	6B	33	79	62	30	61	72	64	34	67	34	dc3tok3yb0ard4g4
000005F0	31	6E	7E	7E	7E	7D	00	00	00	00	01	1B	03	3B	30	00	1n~~~} ;0
00000600	00	00	05	00	00	00	04	FE	FF	FF	7C	00	00	00	44	FE	þÿÿ| Dþ
00000610	FF	FF	4C	00	00	00	31	FF	FF	FF	A4	00	00	00	54	FF	ÿÿL 1ÿÿÿ¤ Tÿ
00000620	FF	FF	C4	00	00	00	C4	FF	FF	FF	0C	01	00	00	14	00	ÿÿÄ Äÿÿÿ
00000630	00	00	00	00	00	00	01	7A	52	00	01	78	10	01	1B	0C	zR x
00000640	07	08	90	01	07	10	14	00	00	00	1C	00	00	00	F0	FD	ð ý
00000650	FF	FF	2A	00	00	00	00	00	00	00	00	00	00	00	14	00	ÿÿ*

最终的答案为：`hctf{scxdc3tok3yb0ard4g41n~~~}`