CTF之MISC套路

原创

sosoxy 于 2020-04-11 17:28:47 发布 2524 收藏 20

分类专栏： 笔记

本文链接：https://blog.csdn.net/qq_45970607/article/details/105453731

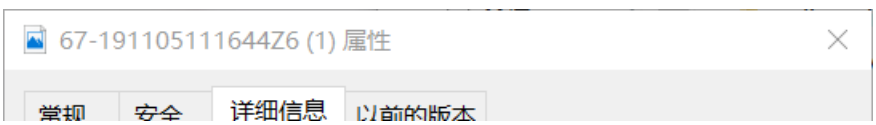
前言

上周做了几个misc题，现在来把它们总结一下。

1.看图片属性

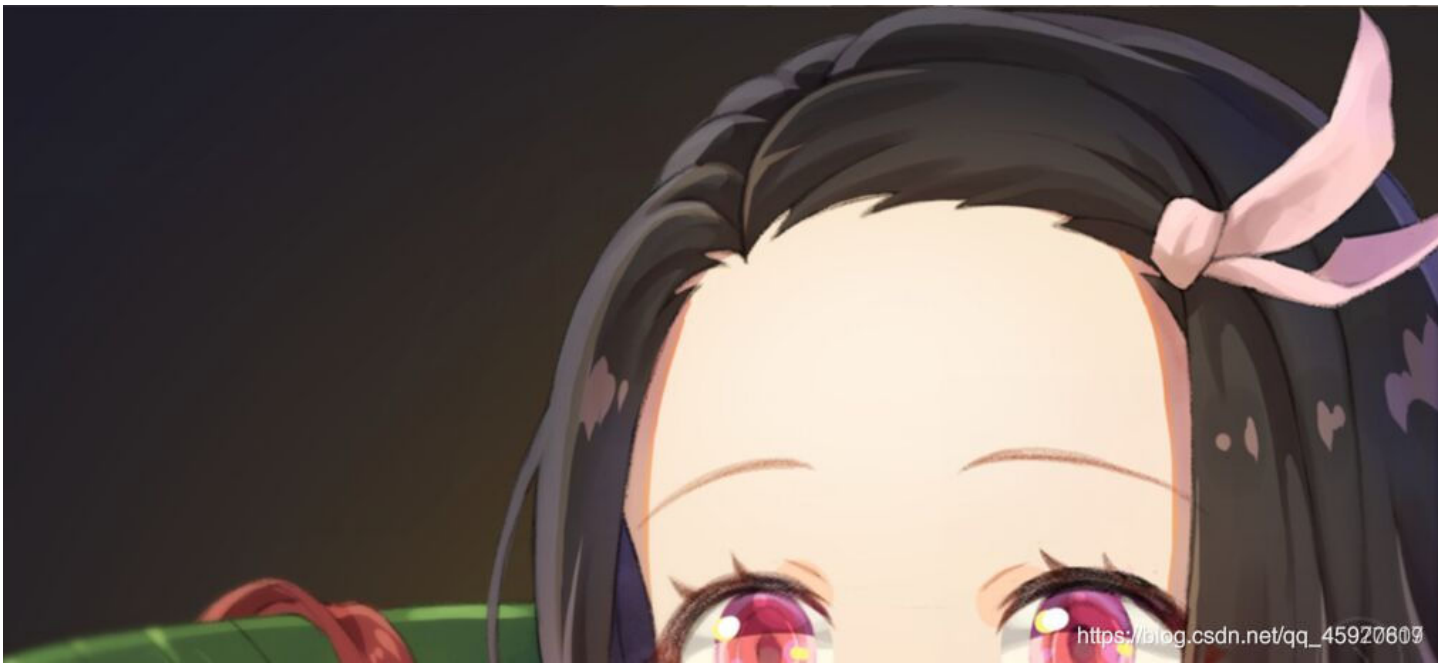
“拿到题记得先看一下图片属性，有时候线索就会隐藏在这里面！”这句话是给我们的做题提示，那么我们就来看一下这张图片的属性，看看有没有我们想要的flag。

我们把这张图片拉到桌面上，然后点击鼠标右键的属性然后我们就会看到关于这张图片的相关信息。然后我们点击第三栏的详细信息，嘿嘿，发现了什么？对，备注里的信息不就是我们想要的flag吗!



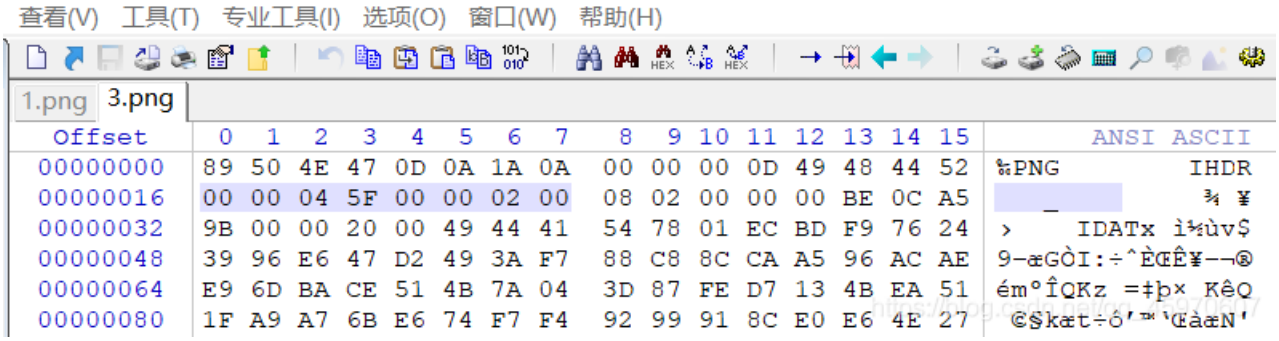
2.修改图片宽或高

题目已经告诉我们要修改图片宽或高，那么我们让图片在winhex里打开，然后修改宽或高就OK了。



我们可以看到这张图片高度好像不完整，所以我们放在winhex里把高度修改一下就可以了，可以看到图中我标记的阴影部分其实

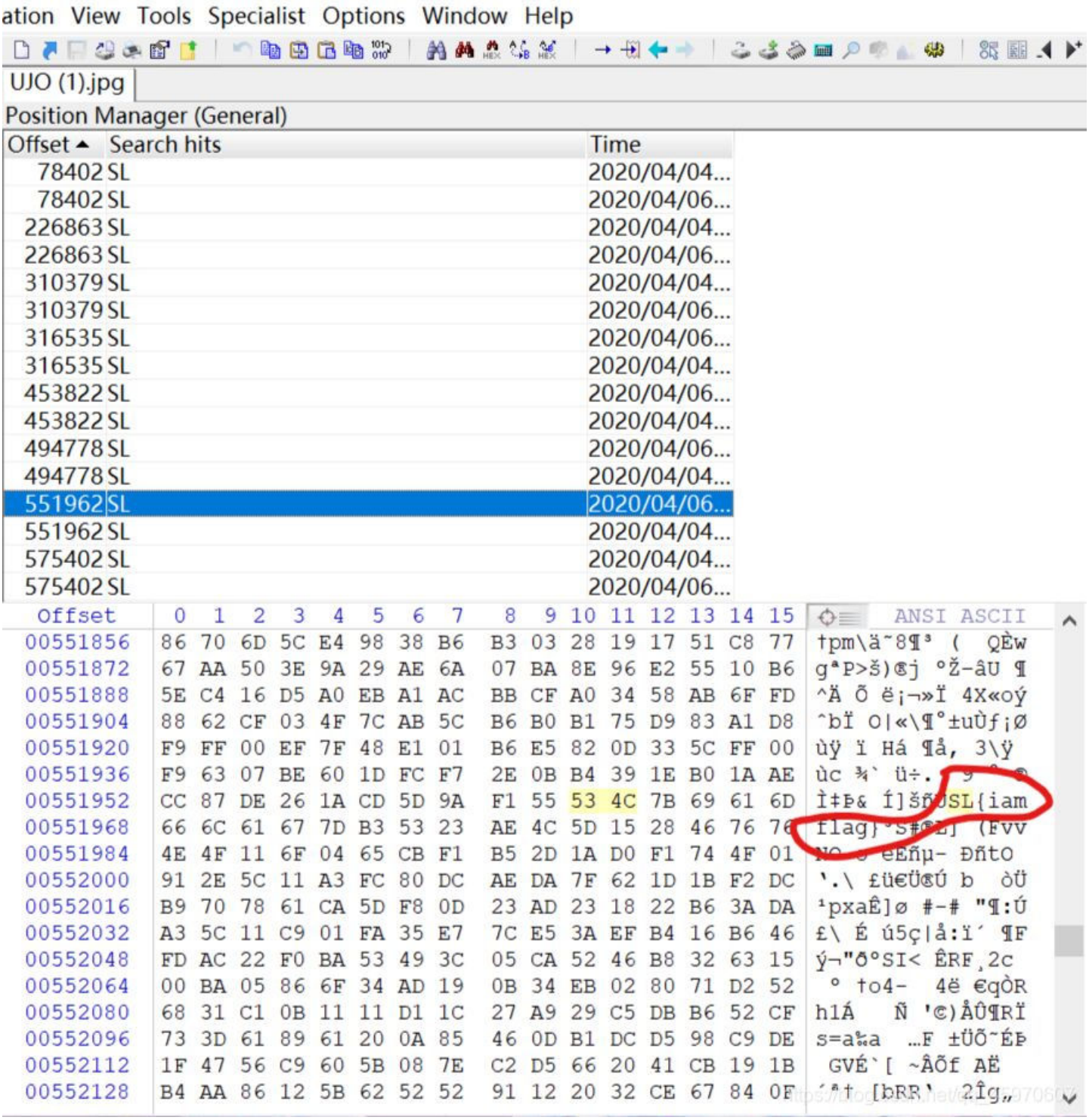
就代表了图片的宽和高，其中前半部分0000045F代表图片的宽，后半部分00000200代表了图片的高，我们需要把代表高的部分00000200修改为和图片的宽0000045F一样就可以了，修改完之后标记的阴影部分就变成了0000045F0000045F，接下来我们按ctrl+s保存图片就可以了。



图片保存之后我们重新打开图片，看一下，然后我们会发现flag就隐藏在还原之后的图片里，最后我们把隐藏在图片里的flag提交就OK了。

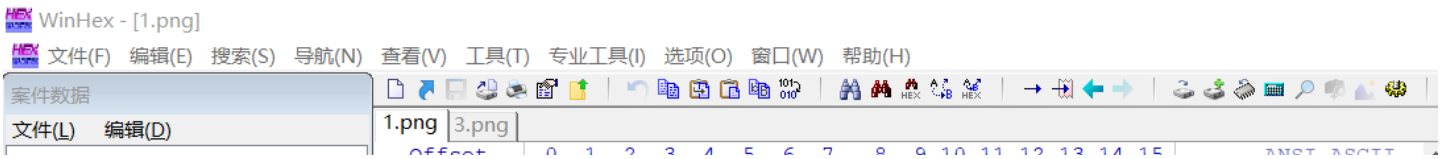
3.SL就隐藏在字节中

同样，这道题给了我们提示信息：“winhex/010 ediot工具要学会去使用，本题格式SL{}”。所以我们直接用winhex打开图片(这里就不再放图片了，直接把图片在winhex里打开 ）。题目告诉我们答题格式为SL{}，那么我们可以按ctrl+f 搜索SL，然后搜索之后图中标记的部分就是答案了。



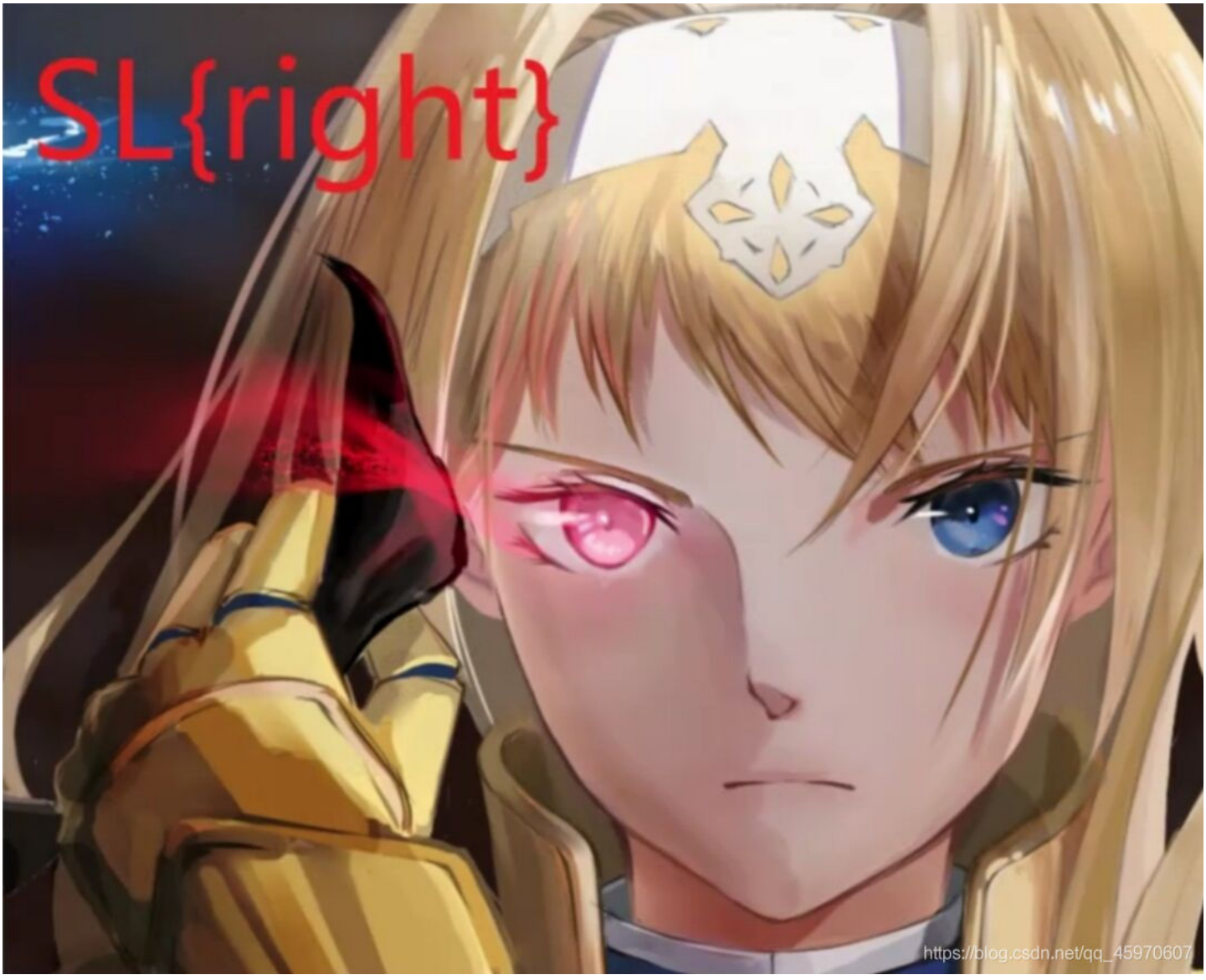
4.补充头部

看到这道题我们应该想到这道题是改文件头的，这道题给我们的图片格式是png，然后把图片放在winhex里边。

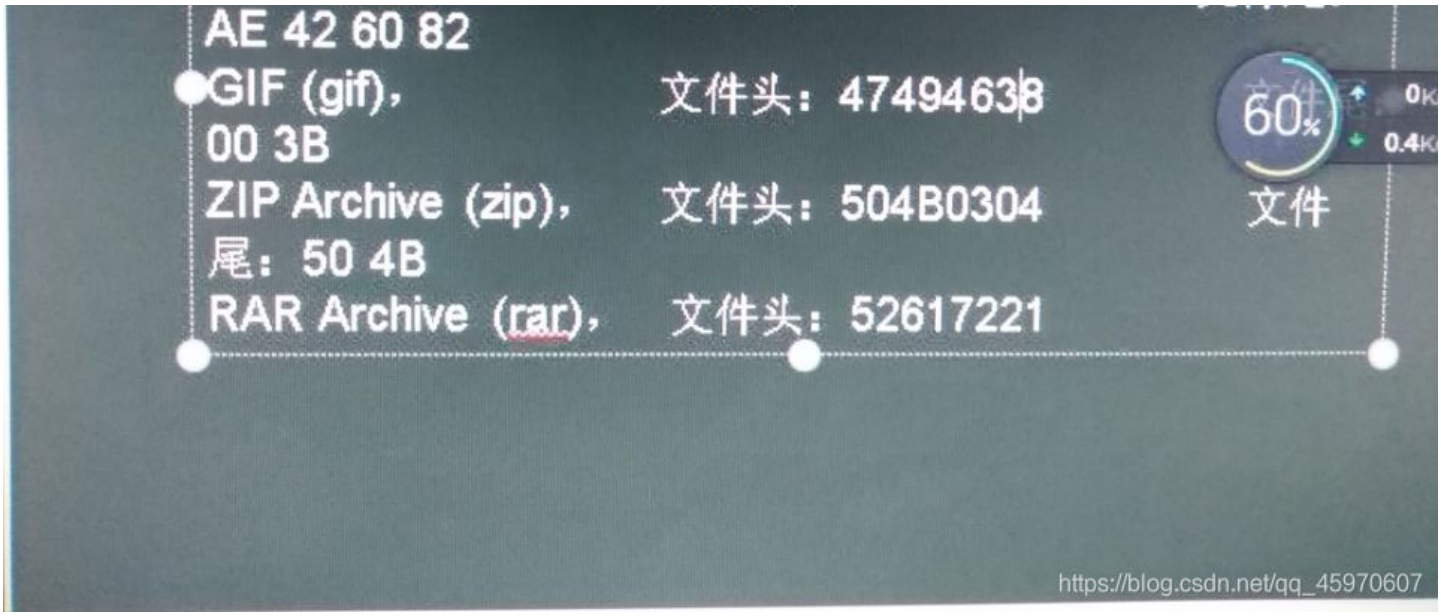


Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
00000000	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	00	00	04	4E	IHDR N
00000016	00	00	03	7B	08	06	00	00	00	5B	2C	DF	1C	00	00	00	{ [,ß
00000032	01	73	52	47	42	00	AE	CE	1C	E9	00	00	00	04	67	41	sRGB ®Î é gA
00000048	4D	41	00	00	B1	8F	0B	FC	61	05	00	00	00	09	70	48	MA ± üa pH
00000064	59	73	00	00	12	74	00	00	12	74	01	DE	66	1F	78	00	Ys t t Þf x
00000080	00	FF	A5	49	44	41	54	78	5E	EC	FD	59	B3	2E	49	B2	ÿ¥IDATx^ìýY³.I²

我们把鼠标光标移到第一行的最前边然后点击右键，然后看到有个编辑，我们点开编辑之后点那个“粘贴0字节”字节数默认4就行，然后我们给文件添加文件头89504E47，然后保存图片就可以在保存后的图片中看到flag了。

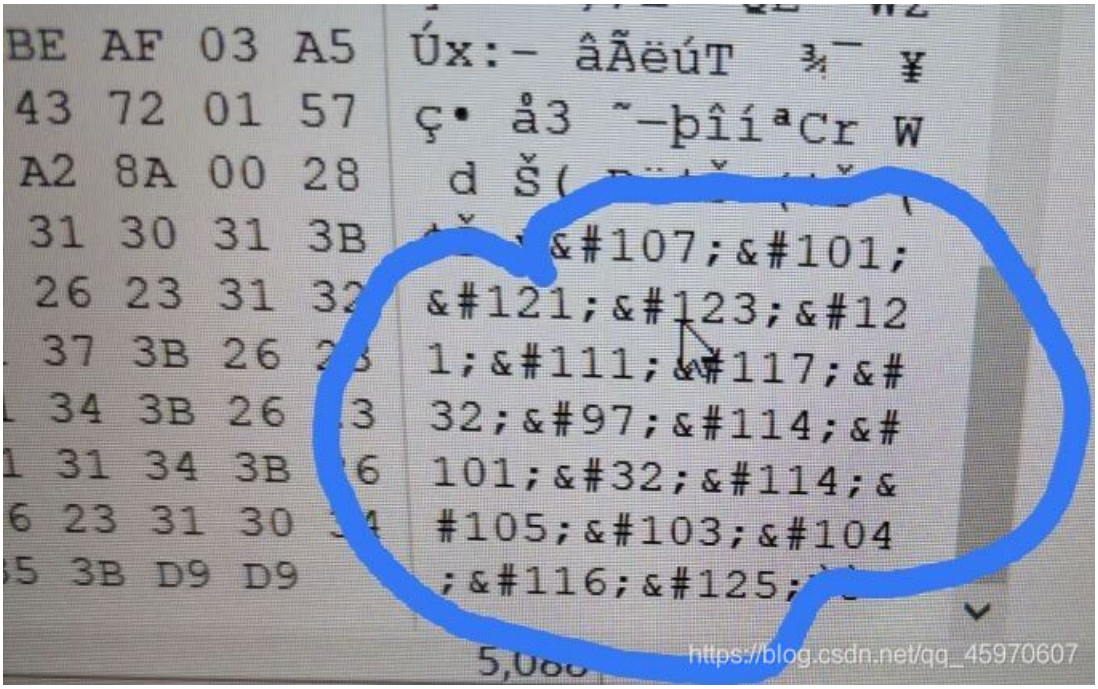


附上一张常见改文件头文件尾格式的图片。



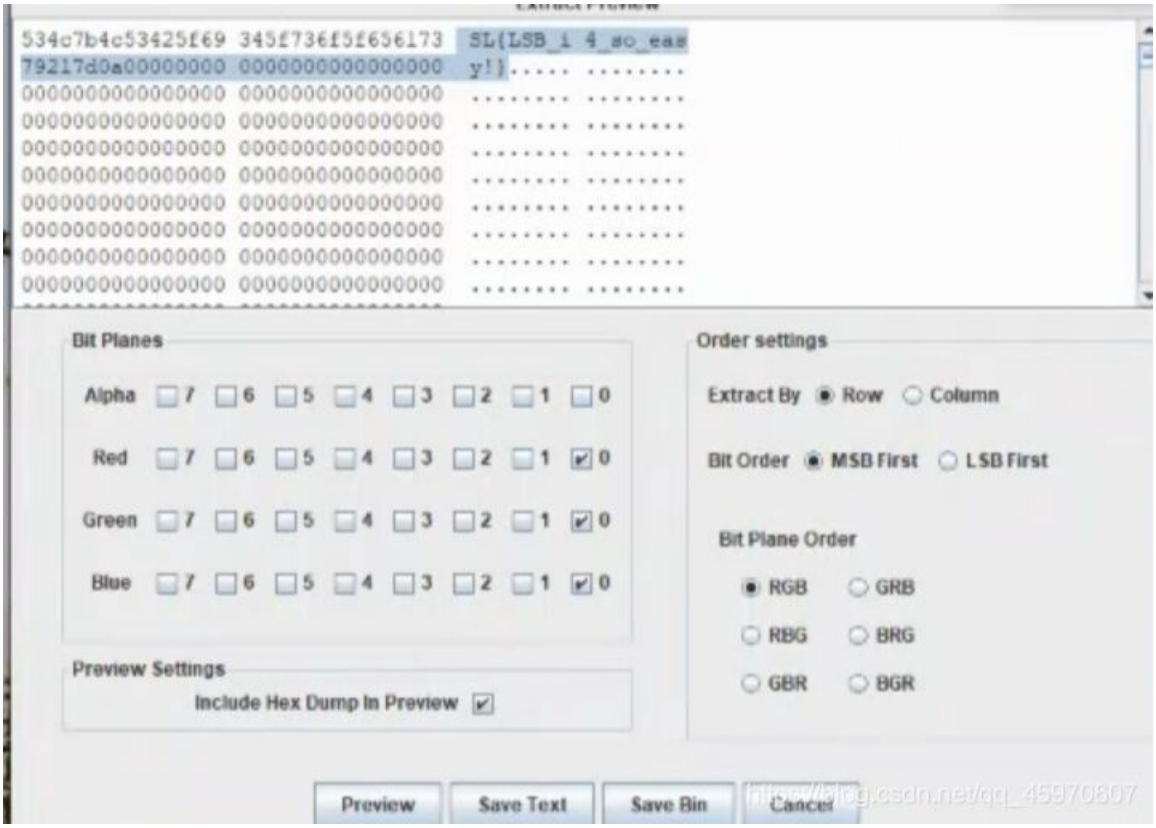
5.签到题

这道题给我们的提示是不要想那么多，它仅仅是一道签到题，所以我们还把它放在winhex里边分析，然后我们拉到最后我们发现我标注的那几行看起来有点让人怀疑，于是我们用ascll码转换器把它解码一下，嘿嘿，没错，解码之后就拿到了flag。



6.LSB

“简单的LSB隐写，在最低有效位隐藏信息。可以使用Stegsolve提取。”哇，这道题又有了明显的提示。于是我们就在Stegsolve里边打开图片（我们在这里就不放图片了）进行分析。打开Stegsolve然后点击Analyse中的第二项 Data Extract 然后我们选中后三列的0通道，选中之后点击Preview显示最低有效位隐藏信息，然后我们就看到了flag。



总结

做完题之后要总结一下，查漏补缺。