

# 攻防世界杂项 SimpleRAR

原创

[Warning](#) 于 2019-05-07 20:40:15 发布 7865 收藏 18

分类专栏: [杂项](#)

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/destiny1507/article/details/89928234>

版权



[杂项 专栏收录该内容](#)

15 篇文章 1 订阅

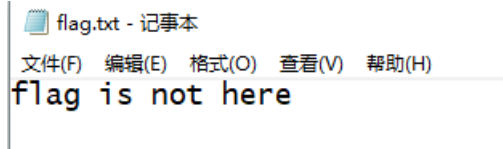
订阅专栏

## SimpleRAR

现在这年头做个杂项还顺便教PS的嘛 (手动微笑)

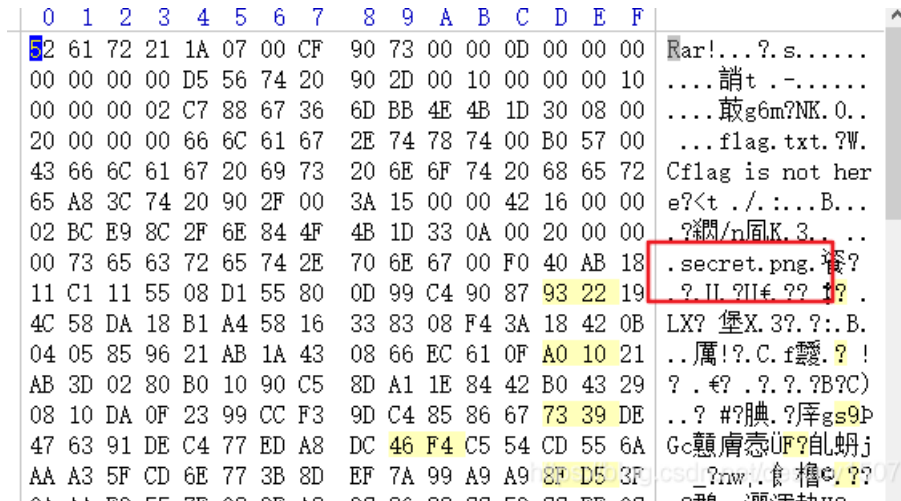
-----正经的分割线

附件是一个RAR压缩包, 解压缩之后只有一个txt文件, 上面写着:



(RAR: 可把我给牛逼坏了)

然后.....例行用winhex打开一发.....发现RAR里面居然是有一个图片的! (怪我过分聪慧哈哈哈哈)



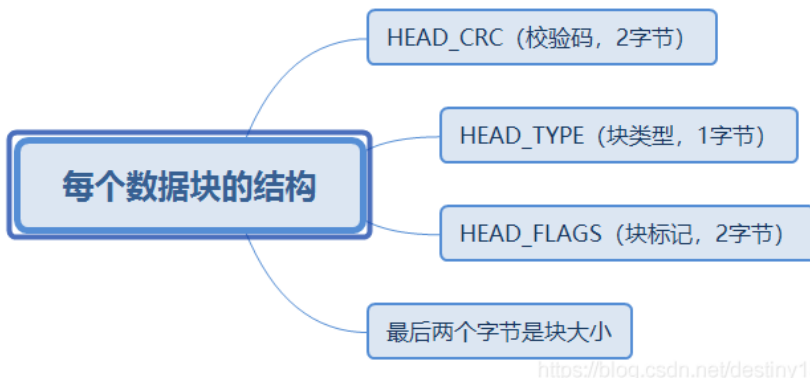
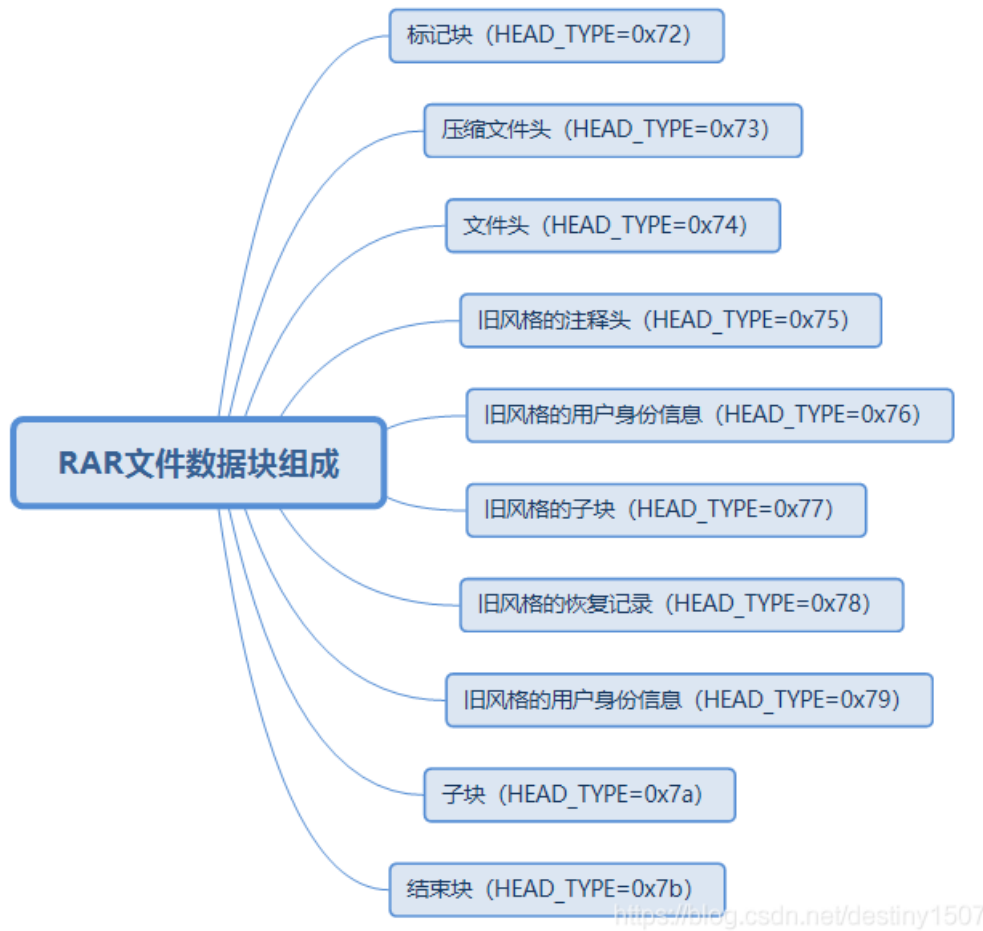
emmmmm可是为什么解压不出来呢? 然后疯狂百度为什么压缩文件里有文件却解压不出来balabala的

后来意识到: 噢, 这个压缩包可能坏掉了.....

HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
000000	52	61	72	21	1A	07	00	CF	90	73	00	00	0D	00	00	00	Rar!...?.s.....
000010	00	00	00	00	D5	56	74	20	90	2D	00	10	00	00	00	10	....請t.-.....
000020	00	00	00	02	C7	88	67	36	6D	BB	4E	4B	1D	30	08	00	....駁g6m?NK.0..
000030	20	00	00	00	66	6C	61	67	2E	74	78	74	00	B0	57	00	...flag.txt.?W.
000040	43	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	Cflag is not her
000050	65	A8	3C	74	20	90	2F	00	3A	15	00	00	42	16	00	00	e?<t ./:....B...
000060	02	BC	E9	8C	2F	6E	84	4F	4B	1D	33	0A	00	20	00	00	.?網/n/K.3. ...
000070	00	73	65	63	72	65	74	2E	70	6E	67	00	F0	40	AB	18	.secret.png.資?
000080	11	C1	11	55	08	D1	55	80	0D	99	C4	90	87	93	22	19	.?.U.?U€.?? †? .

txt文件结束之后就是png文件的开始了，这里我已经改过了，原来好像是A8 3C 7A，这里涉及到RAR文件的结构：

资料参考自<https://wenku.baidu.com/view/918e2c146c175f0e7cd1370d.html> 为了方便阅读，我做成了思维结构图：



因为我们这里是文件头，所以应该是74啦！

修改后重新保存压缩包，果然解压出了一个图片~~

（可惜是个图片纯白的啥子都莫得）

再次用winhex打开这个图片，发现它是一个gif文件，开心地去改了后缀，然后.....然后又陷入了深深的思索.....

之后用Stegsolve打开图片（不管不管反正写杂项没思路就用一堆工具轮着来试，菜鸟本菜鸟了泪）

然后发现了二维码！（开心开心开心



可惜只有一半.....呵，这种猥琐的操作怎么会让我一个聪明机智的21世纪女青年退缩？

.....对没错我想起来了题目中提示的双图层。

然后.....我就开始了漫漫的ps之旅（我真的是在做题吗？？

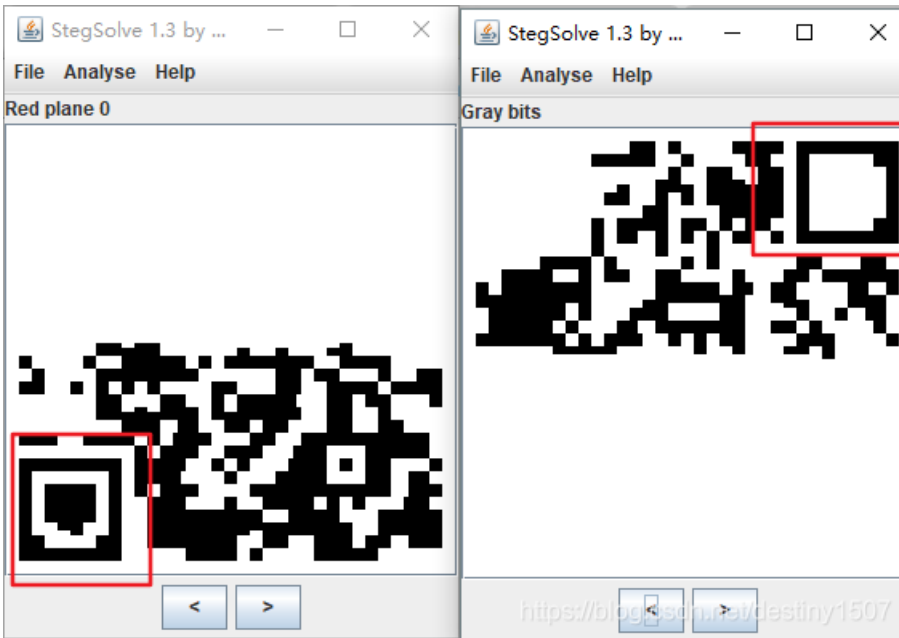
ps纯小白解锁技能：（技能操作就不细写了，百度到处都有

- 用ps分离图层保存
- 抠图
- 合并图片

（问：我为什么这么菜.....

用PS打开那张纯白纯白的secret.gif，果然有两个图层，分离后保存，再用Stegsolve分别打开：

hhhh果然有二维码的上半部分



可惜是个坏掉的.....

可以发现：上半部分的那张图，对于二维码来说右上角最重要的那个小黑块空了，额，左上角索性就根本没有而且，下半部分的那张图，细心点观察也会发现缺掉了一点黑：（我之前就没有注意到，都把二维码补全了死活扫不出来，嚯！



开启抠图技能：既然我们有完整的、没有被破坏的小黑块，那就把它扣过去安在二维码的上半部分试试？

然后两张图片合并就可以了（合并就是把一张的图层复制到另一张图片里）



然后扫描就看到flag啦