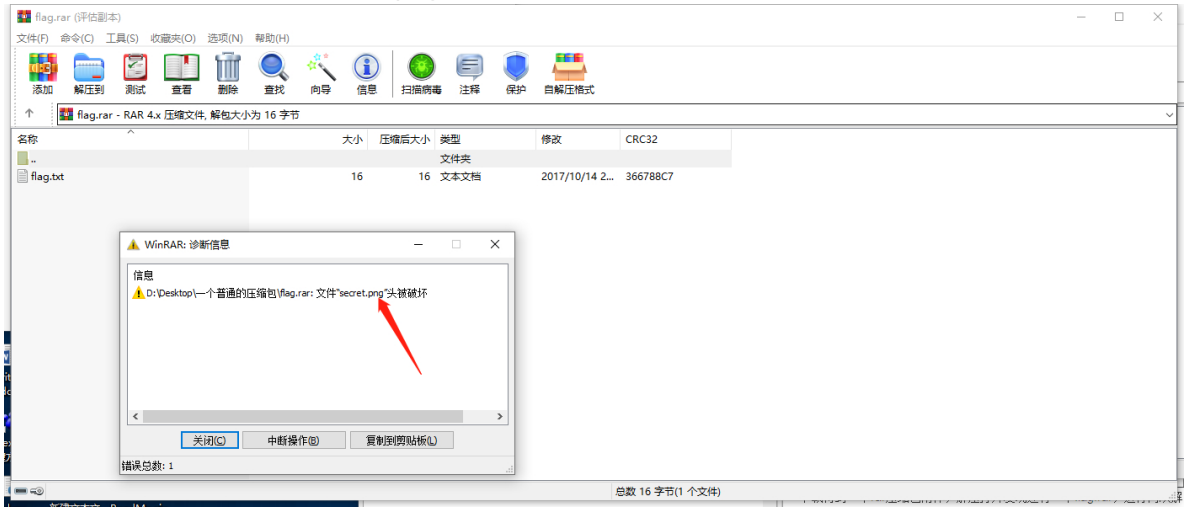
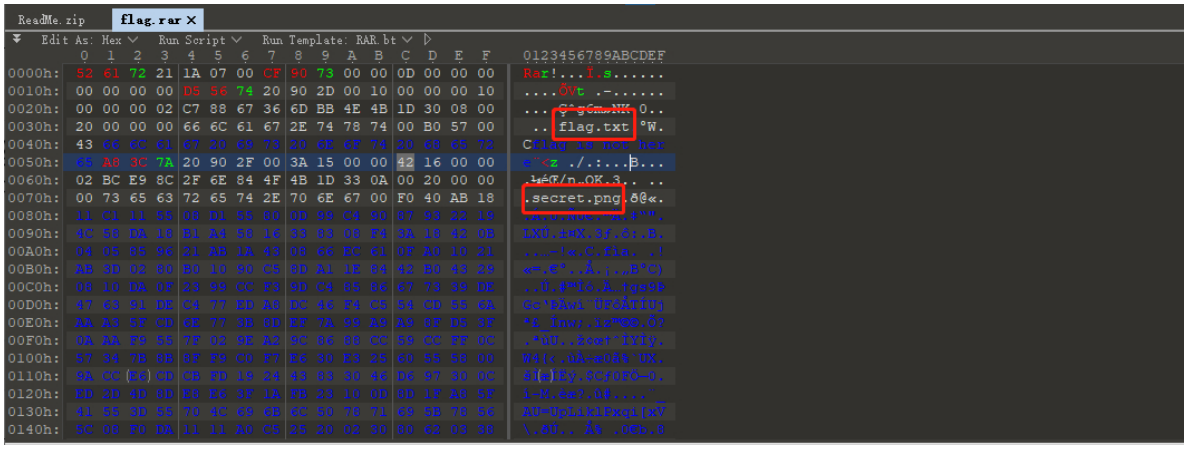
**一个普通的压缩包(xp0intCTF)-writeup**

打开题目


下载得到一个rar压缩包附件，解压打开发现还有一个flag.rar，文件属性，详细信息各种查看确定没有隐藏信息，进行再次解压出现提示png文件损坏

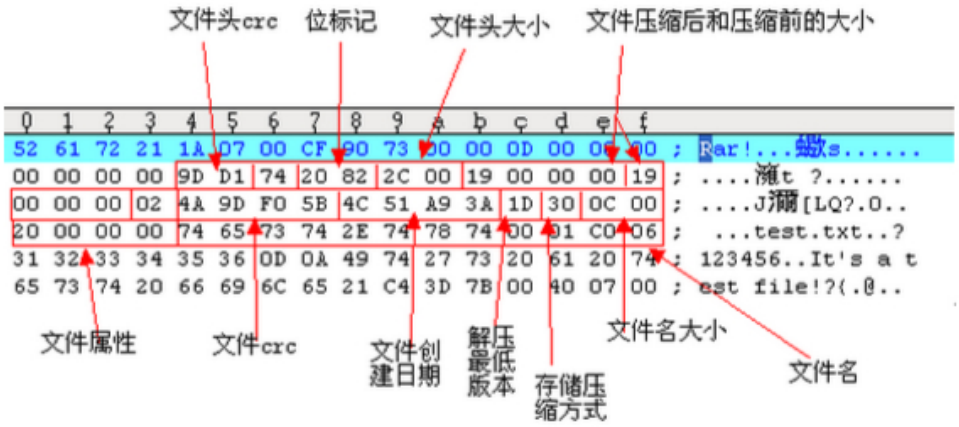



先打开里面的文本看一下，文本内容提示flag is not here，现在把flag.rar放在十六进制工具里看下，发现里面有一张secret.png文件，但是之前提示损坏了，刚开始用winrar自带的修复功能修复不成功，只能自己用010Editor进行手动修复了。

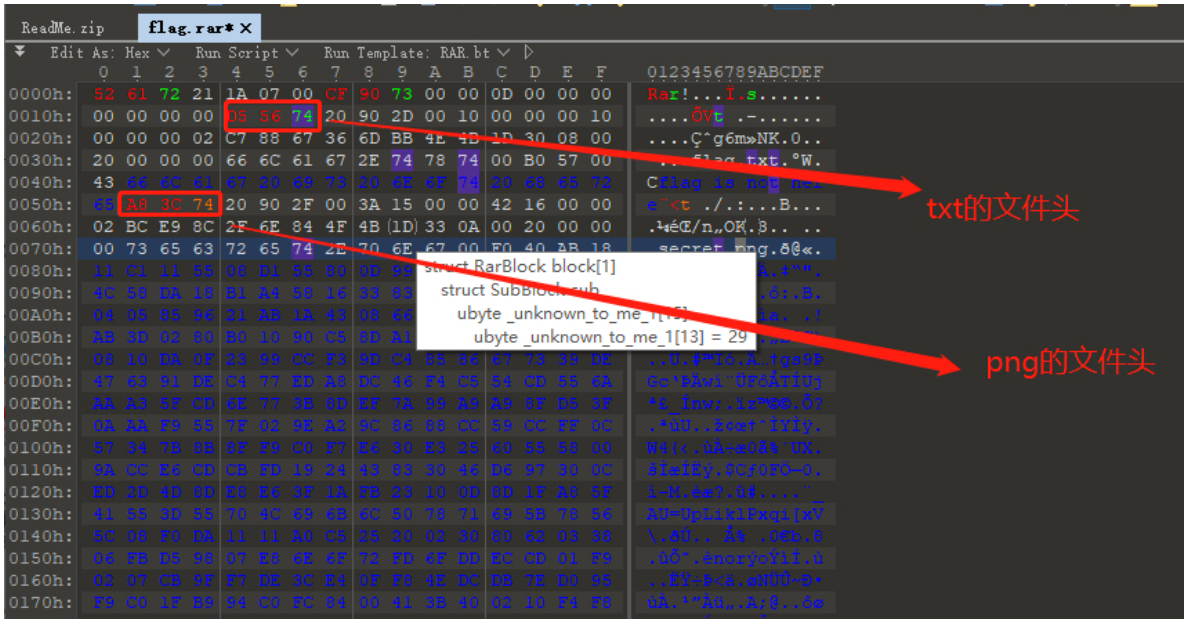


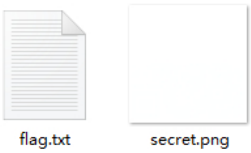

检查rar头，没有问题，然后再看加密部分，检查各个文件的文件头

文件头（FILE_HEAD）
HEAD_TYPE 1 个字节 头类型：0x74



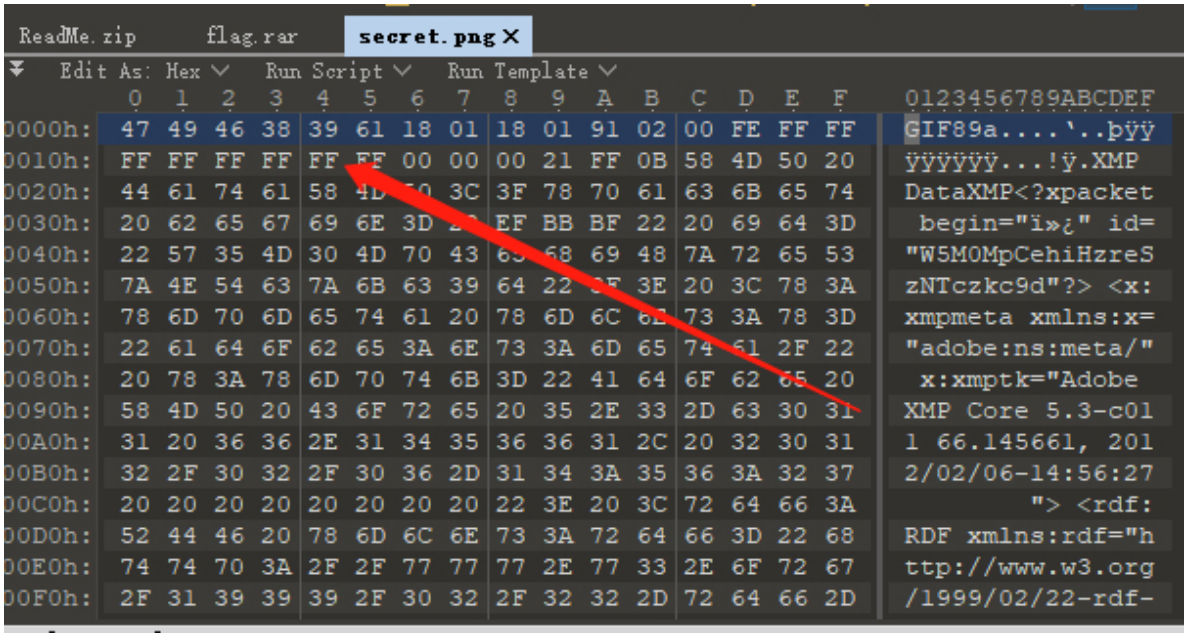

更多可以点击RAR文件格式研究
我们回到我们的题目中来，检查发现png那的文件头类型A8 3C 7A，把7A修改为74，保存，查看是否修复成功。





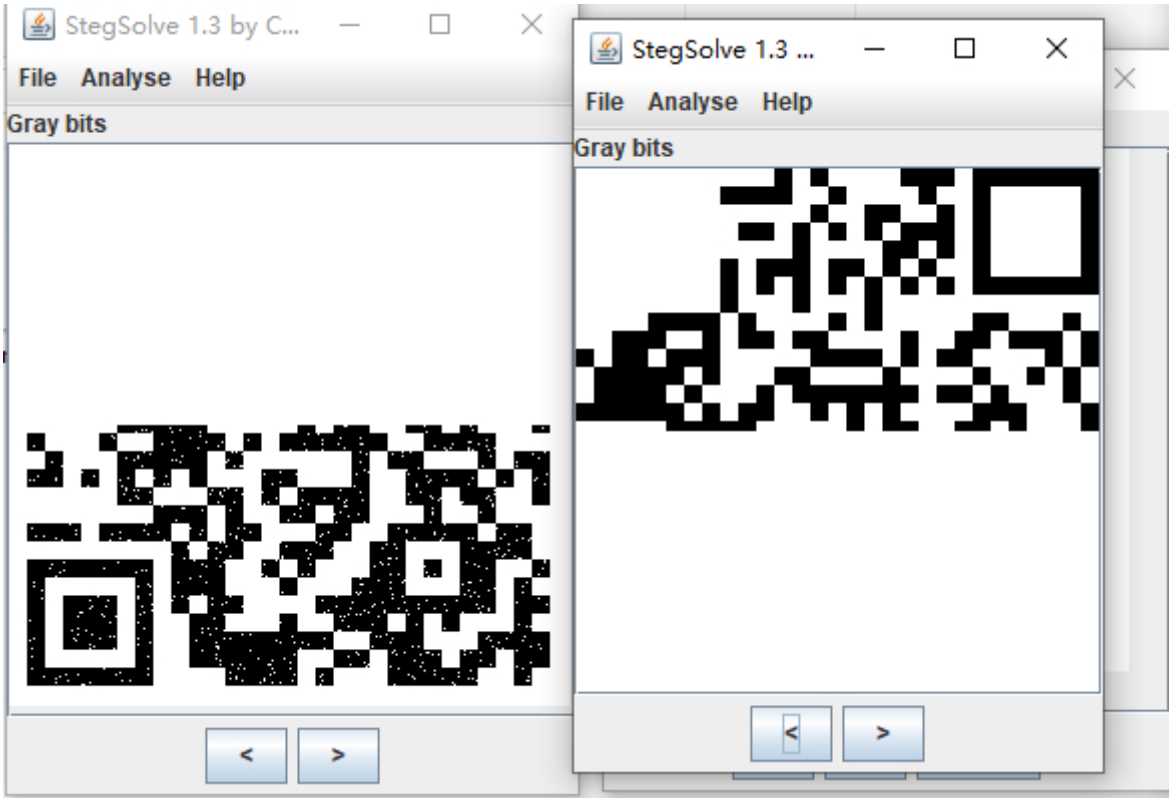

得到secret.png，查看一张纯白的图片，用010Editor查看是一个gif的文件

```
GIF文件头标识 (6 bytes) 47 49 46 38 39(37) 61-- GIF89(7)a
```

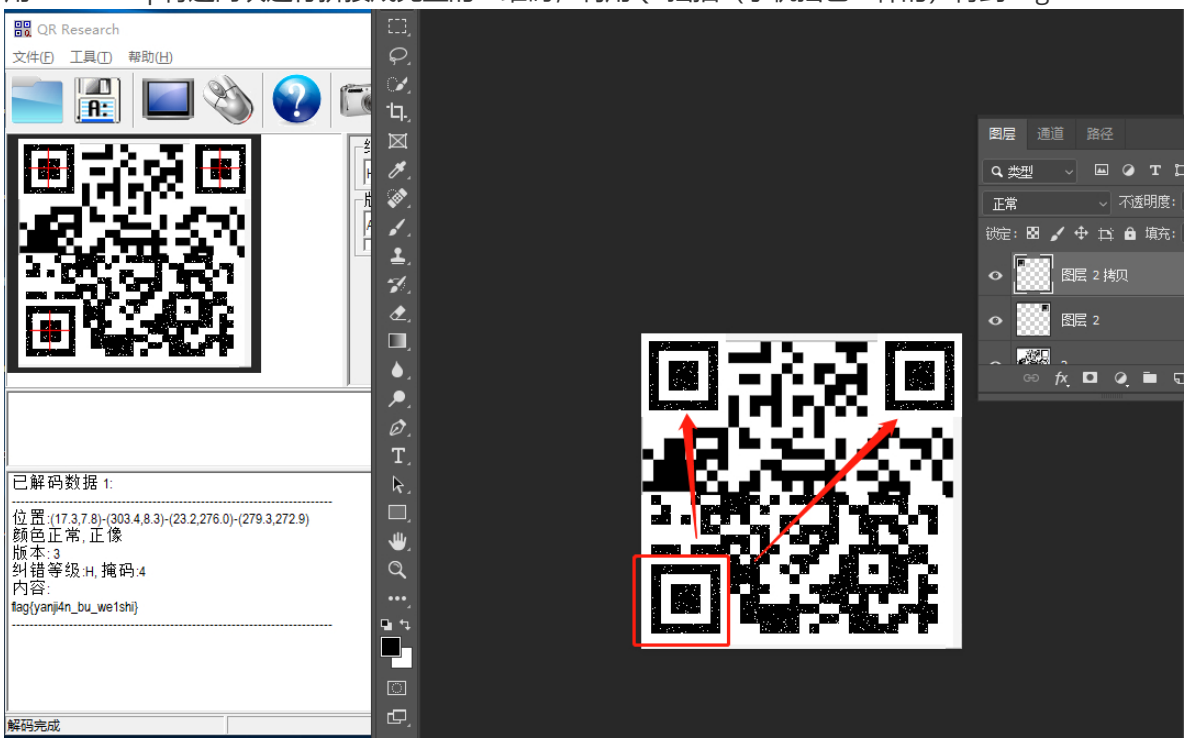



修改为gif用stegsolve查看得到gif的两帧每一帧有半张二维码(这里也可以用Photoshop进行分离图层)

```
StegSolve
Analyse下面几个功能键作简单介绍：
File Format:文件格式，这个主要是查看图片的具体信息
Data Extract:数据抽取，图片中隐藏数据的抽取
Frame Browser:帧浏览器，主要是对GIF之类的动图进行分解，动图变成一张张图片，便于查看
Image Combiner:拼图，图片拼接
```




用Photoshop将这两块进行拼接成完整的二维码，利用QR扫描（手机扫也一样的）得到flag




二维码的生成细节和原理有兴趣的可以去了解下。