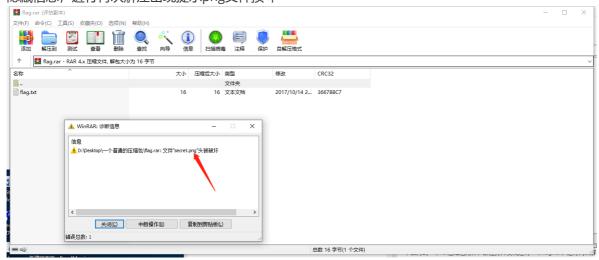
一个普通的压缩包(xp0intCTF)-writeup

打开题目



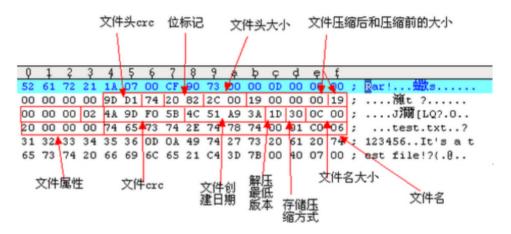
下载得到一个rar压缩包附件,解压打开发现还有一个flag.rar,文件属性,详细信息各种查看确定没有隐藏信息,进行再次解压出现提示png文件损坏



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。

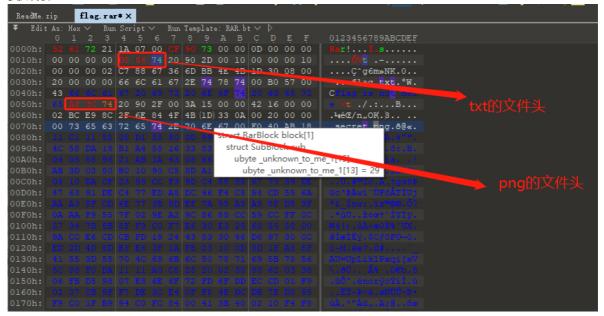
检查rar头,没有问题,然后再看加密部分,检查各个文件的文件头

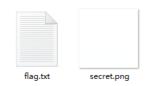
```
文件头(FILE_HEAD)
HEAD_TYPE 1 个字节 头类型: 0x74
```



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

```
ReadMe. zip
            flag.rar
                      secret.png X
                Run Script 🗸
                            Run Template 🗸
                                                          0123456789ABCDEF
      47 49 46 38 39 61 18 01 18 01 91 02 00 FE FF FF
                                                          GIF89a....\..bÿÿ
0010h: FF FF FF FF FF FF 00 00 00 21 FF 0B 58 4D 50 20
                                                          ÿÿÿÿÿÿ...!ÿ.XMP
                          3C 3F 78 70 61 63 6B 65 74
0020h: 44 61 74 61 58 4D
                                                          DataXMP<?xpacket
0030h: 20 62 65 67 69 6E 3D 2
                              EF BB BF 22 20 69 64 3D
                                                           begin="i»¿" id=
0040h: 22 57 35 4D 30 4D 70 43 63
                                  68 69 48 7A 72 65 53
                                                          "W5M0MpCehiHzreS
0050h: 7A 4E 54 63 7A 6B 63 39 64 22
                                      E 3E 20 3C 78 3A
                                                          zNTczkc9d"?> <x:
      78 6D 70 6D 65 74 61 20 78 6D 6C 61
                                          73 3A 78 3D
                                                          xmpmeta xmlns:x=
                               73 3A 6D 65 74
070h: 22 61 64 6F 62 65 3A 6E
                                               61 2F 22
                                                          "adobe:ns:meta/"
0080h: 20 78 3A 78 6D 70 74 6B 3D 22 41 64 6F 62 65 20
                                                           x:xmptk="Adobe
                                                          XMP Core 5.3-c01
00A0h: 31 20 36 36 2E 31 34 35 36 36 31 2C 20 32 30 31
                                                          1 66.145661, 201
DOBOh: 32 2F 30 32 2F 30 36 2D 31 34 3A 35 36 3A 32 37
                                                          2/02/06-14:56:27
00C0h: 20 20 20 20 20 20 20 20 28 22 3E 20 3C 72 64 66 3A
                                                                  "> <rdf:
DODOh: 52 44 46 20 78 6D 6C 6E 73 3A 72 64 66 3D 22 68
                                                          RDF xmlns:rdf="h
DOEOh: 74 74 70 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72 67
                                                          ttp://www.w3.org
00F0h: 2F 31 39 39 39 2F 30 32 2F 32 32 2D 72 64 66 2D
                                                          /1999/02/22-rdf-
```

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

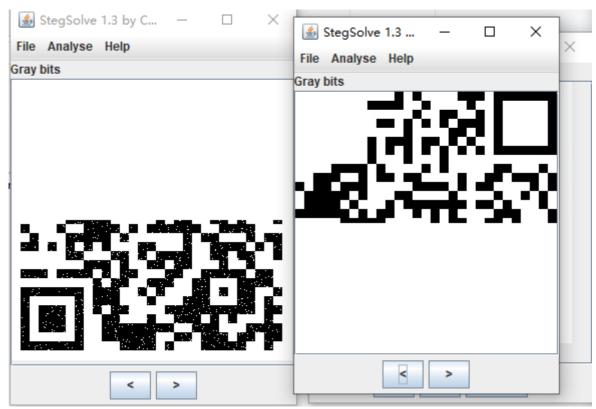
Analyse下面几个功能键作简单介绍:

File Format:文件格式,这个主要是查看图片的具体信息

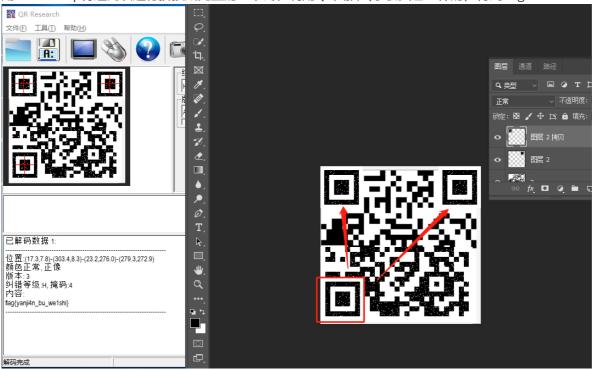
Data Extract:数据抽取,图片中隐藏数据的抽取

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。