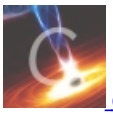
misc隐写学习

原创

Pz1o 于 2020-05-06 20:55:38 发布 460 收藏 1

分类专栏： ctf 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_45679095/article/details/105958928



文章目录

图片隐写

1.基础知识

文件格式

PNG格式通常由文件头和数据块构成。

文件头: *89 50 4E 47 0D 0A 1A 0A* + 数据块+数据块+数据块

其中数据块由两个部分构成，第一种是**关键数据块**，是标准数据块；第二种是**辅助数据块**，是可选数据块。关键数据块定义了4个标准数据块，PNG文件必须包含。

文件头数据块(IHDR)、图像数据块(IDAT)、图像结束数据块(IEND)这三部分是不可省略的。

对于每个数据块都有着统一的数据结构，每个数据块由4个部分组成。

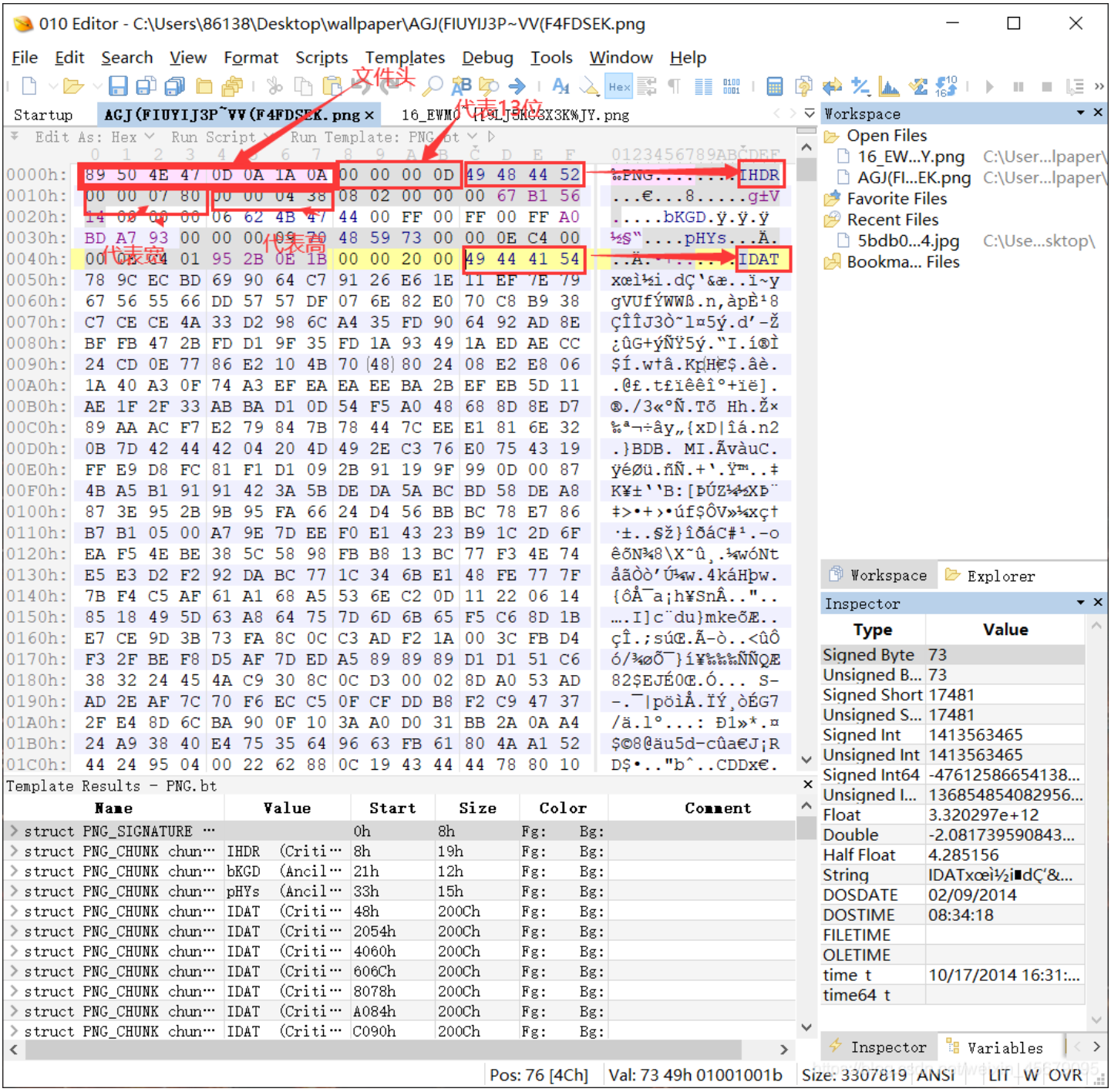
名称	字节数	说明

名称	字节数	说明
length	4	指定数据块数据域长度
Chunk Type Code(数据块类型码)	4	由ASCII中A-Z和a-z祖成
Chunk Data(数据块数据)	可变	存储按照CTC指定的数据
CRC(循环冗余检测)	4	用来检测错误的循环冗余码

IHDR(文件头数据块)

文件头数据块，它包含有PNG文件中存储的图像数据的基本信息，由13字节组成，并要作为第一个数据块出现在PNG数据流中，而且一个PNG数据流中只能由一个文件头数据块，前八字节内容如下

域的名称	字节数	说明
Width	4	图像宽度
Height	4	图像高度



元数据

元数据又叫中介数据、中继数据，为描述数据的数据，主要是描述**数据属性**的信息，用来支持如指示存储位置、历史数据、资源查找、文件记录等功能。

windows->右键->属性查看

Linux->直接使用exiftool查看

2.隐写

图片长宽，信息隐藏

改变图片中IHDR的宽和高达到显示信息的目的。

图片中追加内容

在图片尾部追加文字，压缩包和一些其他文件

IEND找到图片结尾的标识，分离文件即可

strings：打印一些字符，从而发现在压缩包中的内容和密码。

IDAT信息隐藏

IDAT：存储实际的数据，在数据流中可包含多个连续顺序的图像数据块。存储图像像素数据。采用LZ77算法的派生算法进行压缩，可以用python中的zlib模块解压缩

- IDAT块只有当上一个块充满时，才会继续下一个新块,所以只有一个未满的IDAT
- 可以用stegsolve->Format Analysis查看详细信息

LSB图片隐写

PNG文件中的图像像数一般是由RGB三原色组成，每一种颜色占用8为，取值范围为0x00-0xff，即256钟颜色，所以共包含了256^3种颜色。

LSB隐写就是修改RGB颜色分量的最低二进制位。

RGB(218,150,149)

R=11011010;

G=10010110;

B=10010101;

量的最低二进制位。

RGB(218,150,149)

R=11011010;

G=10010110;

B=10010101;

修改R=11011011;