文件隐写方法与思路汇总

原创

奥斯科AUSCOO 于 2020-10-23 11:26:00 发布 577 收藏 1
文章标签： python java 机器学习 人工智能 算法

本文链接：https://blog.csdn.net/Auscoo111/article/details/109253216

文件隐写方法与思路汇总

```
JPEG
    JPEG 是Joint Photographic Experts Group(联合图像专家小组)的缩写，是第一个国际图像压缩标准。JPEG图像压缩算法能够在
    JPEG本身只有描述如何将一个影像转换为字节的数据串流(streaming)，但并没有说明这些字节如何在任何特定的储存媒体上被封存起
    在各种图像格式中JPEG是使用非常广泛的一种，用JPEG图像作为载体进行信息隐藏将不容易引起拦截者发现，因此JPEG信息隐藏具有
    F5算法F5是由德国著名学者Pfitzmann和Westfeld在2001年提出的一种隐写分析方法，是一种针对JPEG图像，可以提供较大的嵌入容
    1、由用户输入的密码产生一组随机序列，利用该随机序列来随机选择量化DCT系数的非零交流系数。
    2、对选中的DCT系数进行分组，每组包含2k-1个DCT系数，用以嵌入k比特秘密信息。
    3、利用矩阵编码来嵌入信息。
```

```
BMP
    BMP图像用作信息隐藏可以隐藏较大的信息量，相对检测难度也较大，可以说BMP图像是信息隐藏的极佳载体。针对文件结构的信息隐藏
    BMP(Bitmap-File)图形文件是Windows采用的常见图形文件格式，要利用BMP位图进行信息隐藏首先需要详细了解BMP文件的格式，B
    在不影响图像正常显示情况下，可使用以下四种方法在24位真彩色BMP图像中隐藏信息。
    1、在图像文件尾部添加任意长度的数据，秘密信息存放在文件尾部可以减少修改文件头的数据量，仅需修改文件头中文件长度的值即可
    2、在调色板或者位图信息头和实际的图像数据之间隐藏数据，如果将秘密数据放在文件头与图像数据之间，则至少需要修改文件头中文
    3、修改文件头和信息头中的保留字段隐藏信息。
    4、在图像像素区利用图像宽度字节必须是4的倍数的特点，在补足位处隐藏数据。
```

```
MP3
    MP3Stego是剑桥大学计算机实验室安全组开发的一个公开源代码的免费程序，它是在MP3上进行水印嵌入研究的最具有代表性的软件。
    数字音频的频域信号在量化和编码时，存在量化误差。这个量化误差是一个不确定值，例如采用不同的心理声学模型可以导致不同的量
```

根据水印被加载的时刻，软件水印可分为静态软件水印和动态软件水印。

1、静态软件水印

静态软件水印的存在不依赖于软件的运行状态，可以在存放、分发以及运行时被验证。静态软件水印在软件编码时或编码完成后被直接

(1)静态数据水印

这类软件水印处于程序流程之外，因此通常存放在软件的固定数据区(data segment)，这种水印验证方法往往比较简单，一般软件会

(2)静态代码水印

这类水印一般存放在软件的可执行流程之中，通常的办法是放在一些不会被执行到的分支流程内，比较典型的就是放在一系列比较判断

2、动态软件水印

软件水印存在依赖于软件的运行状态，通常是在某种特殊的输入下触发才会产生，其验证也必须在这类特定时机才可完成。根据水印产

(1)Easter Egg

在软件接收某种特殊输人时，会显示出指定的一些信息，如软件所有者的照片，软件开发公司的标识等等。

(2)动态数据结构水印

在一段特殊输人的触发下，软件内部会初始化或建立某一特定的数据结构以表示软件的知识产权，验证水印必须在运行时观察到这类数

(3)动态执行序列水印

在接收到一类特殊的输人触发后，软件内部的执行序列会表现出一系列独有的特征，这类特征可以用来作为软件的知识产权标志。

解密网站

如果给一张图片，通常背后有一串被加密或者是flag。这里就需要图片解析工具来解析。解析后的文件输出到txt文件中，再进一步分析。

http://tool.chinaz.com/tools/textencrypt.aspx

培根密码解码过程

第一步：查看实验工具文件夹下面的
Pcat.jpg
图片，发现是一张二维码，手机扫描
(扫描后进入该博客，复制该博客的链接)
第二步：该博客的链接便是扫描后的字符串，发现是网址格式，但是大小写搭配随意，去掉特殊字符后，发现 一共二十个字符，推测培根密码
培根密码有两种解密方式：
第一种解密方式：
A aaaaa B aaaab C aaaba D aaabb
E aabaa F aabab G aabba H aabbb
I abaaa J abaab K ababa L ababb
M abbaa N abbab O abbba P abbbb
Q baaaa R baaab S baaba T baabb
U babaa V babab W babba X babbb
Y bbaaa Z bbaab
第二种解密方式：
a AAAAA g AABBA n ABBAA t BAABA

b AAAAB h AABBB o ABBAB u-v BAABB
c AAABA i-j ABAAA p ABBBA w BABAA
d AAABB k ABAAB q ABBBB x BABAB
e AABAA l ABABA r BAAAA y BABBA
f AABAB m ABABB s BAAAB z BABBB
我们在此处将20个字符分为四组，每组五个，大写为B，小写为A，得到如下：
HttPp→BAABA→t
catcn→AAAAA→a
bloGs→AAABA→c
cOMHh→ABBBA→p
得到密码为：tacp

文件分离

如果图片中有图片重叠，可以使用Kali中的

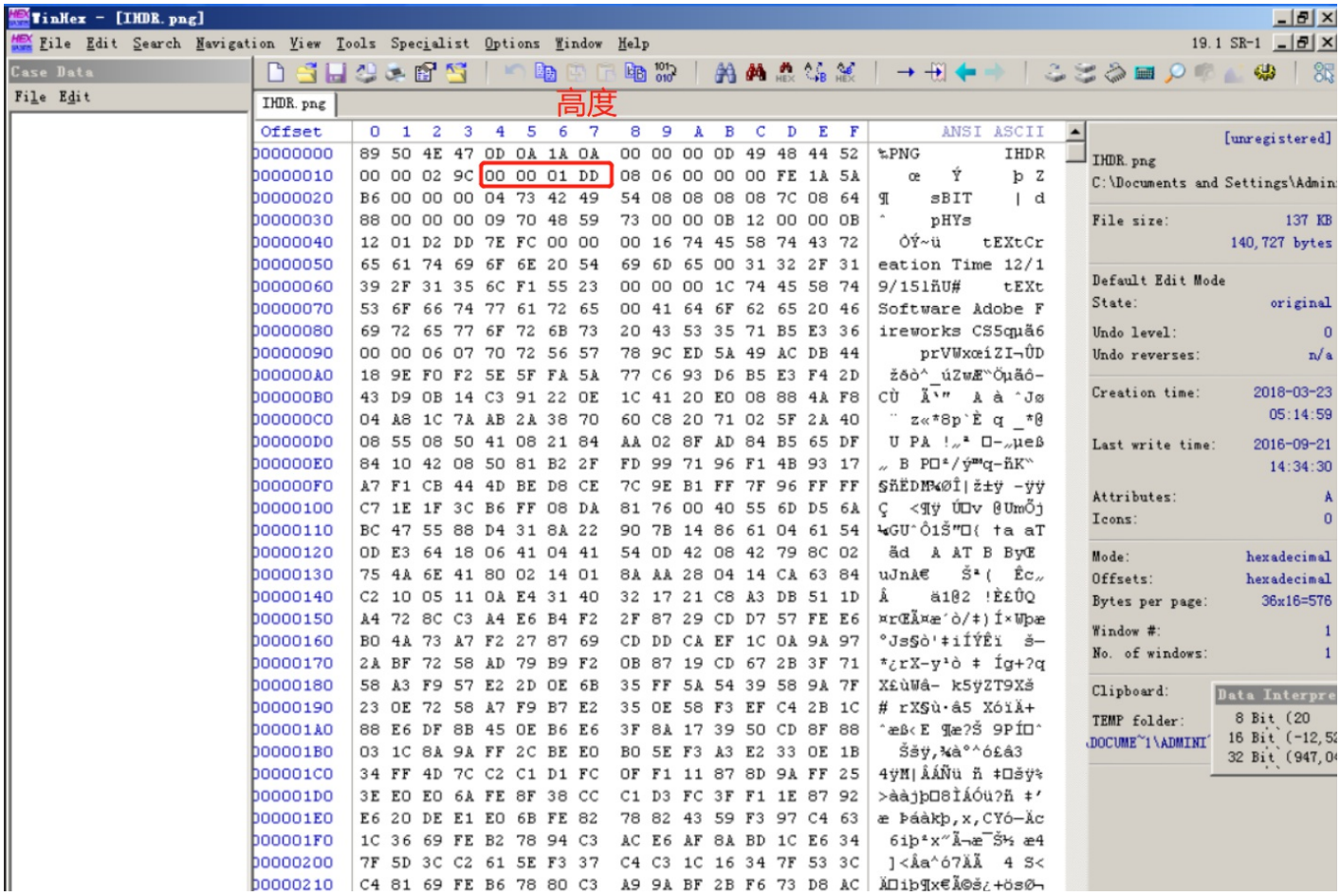
1、进入kali
打开终端用 **binwalk**查看文件格式。
可以直接把桌面的 **oddpic.jpg**拖动到终端(黑框框)里。会变成'/root/桌面/oddpic.jpg'
2、用 **foremost**分离，运行:foremost -v -i 图片路径 -o test
3、分离出了两张图片(在文件夹test中)

图片隐写

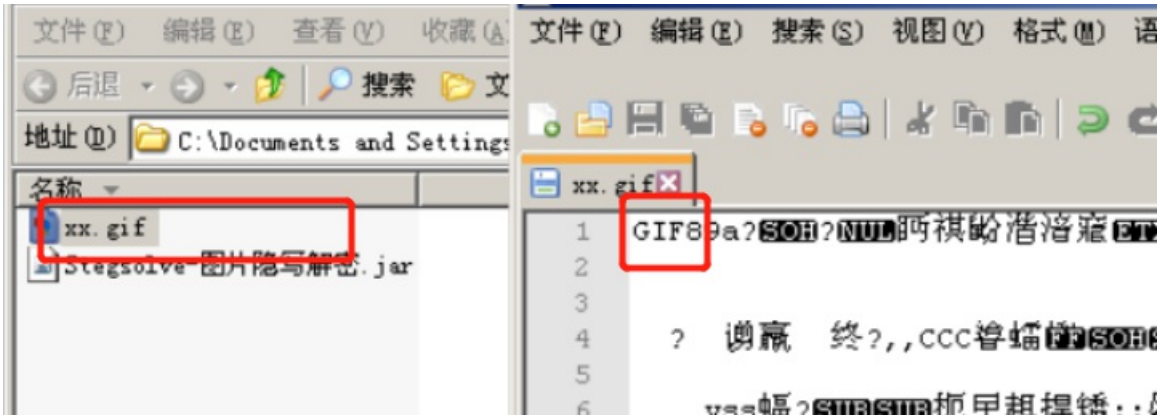
```
. /outguess -r angrybird.jpg outfile.txt
cat outfile.txt
```

PNG图片类型

十六进制值	描述
00 00 00 0D	文件头的数据长度，00 00 00 0D =13
49 48 44 52	数据块类型标志，49 48 44 52 的 ASCII 值等于 IHDR
00 00 02 9C	图像的宽度
00 00 01 DD	图像的高度
08	色深，表示 2 的 8 次幂等于 256 色
06	06 表示索引图像
00	00 表示使用 Deflate 压缩编码压缩图像数据
00	00 表示为将来使用更好的压缩方法预留
00	00 表示非隔行扫描

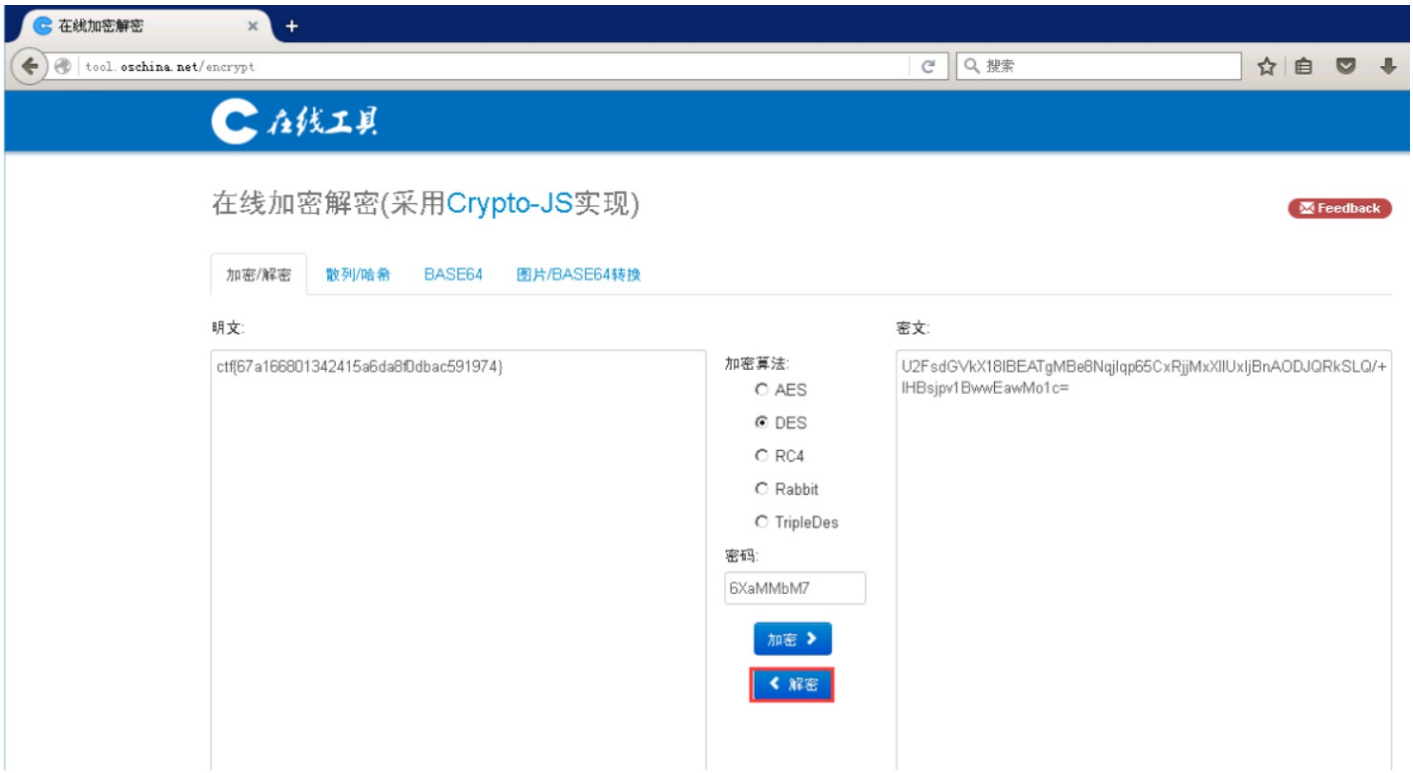


图片修复



图片组合

扫描三个二维码可以得到以下三个结果：
DES
6XaMMbM7
U2FsdGVkX18lBEATgMBe8Nqjlqp65CxRjjMxXllUxljBnAODJQRkSLQ/+lHBsjpv1BwwEawMo1c=
这样就非常清楚了，第一个二维码是加密方式，第二个是密钥，第三个是密文。
第十步：进入
https://tool.oschina.net/encrypt


在线加密解密
tool.oschina.net/encrypt
搜索
在线工具
在线加密解密(采用Crypto-JS实现)
Feedback
加密/解密
散列/哈希
BASE64
图片/BASE64转换
明文:
ctf{67a166801342415a6da8f0dbac591974}
加密算法:
AES
DES
RC4
Rabbit
TripleDes
密码:
6XaMMbM7
加密
解密
密文:
U2FsdGVkX18IBEATgMBe8NqjIqp65CxRjjMxXIIUxIjBnAODJQRkSLQ/+IHBsjpv1BwwEawMo1c=