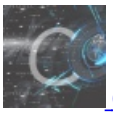
ctf竞赛隐写术分析工具简述

原创

yh野良 于 2020-11-06 18:52:47 发布 261 收藏 1

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/weixin_46065653/article/details/109536852



ctf竞赛隐写术分析工具简述

隐写术，即隐藏书写的信息的技术隐写术属于信息隐藏技术当中的一种，旨在保护秘密信息的安全传输。

ctf比赛中隐写术现状

拿到图片后大致从以下三个方面入手

①Binwaik＋winhex方向

②StegSolve方向

③StegDetect方向

比赛时如果没有解题思路可以依次尝试各个解法。

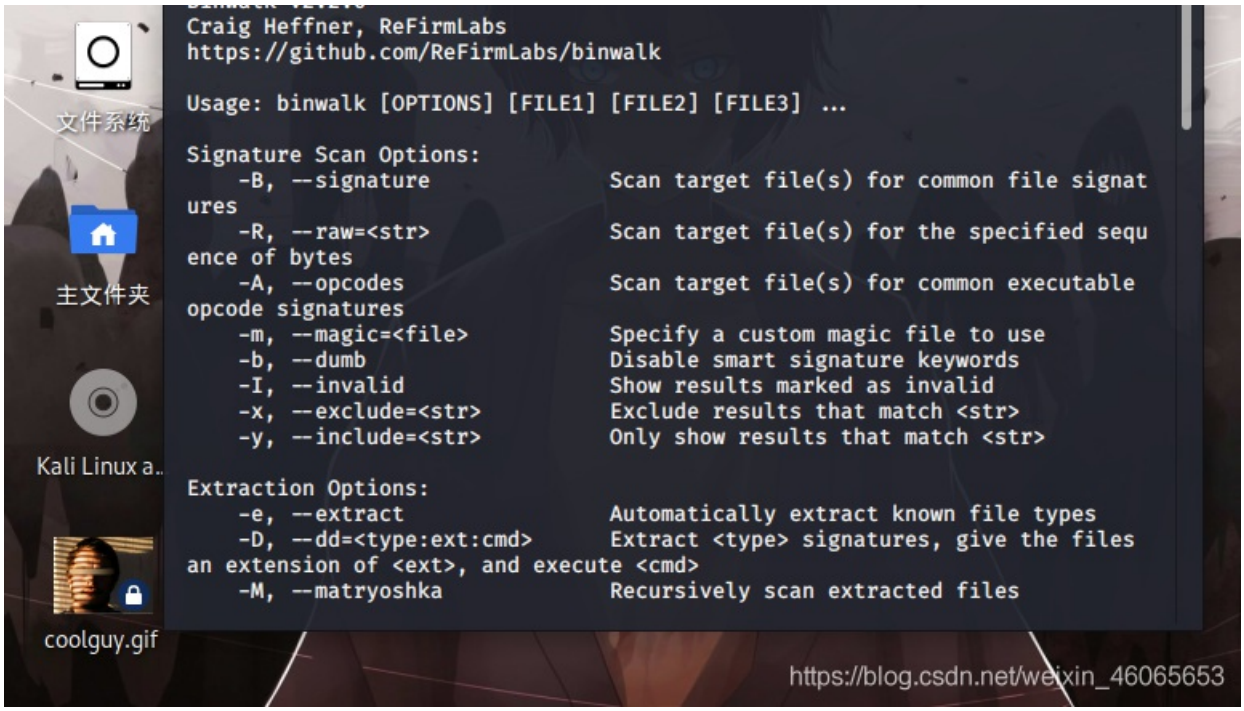
Binwalk （kail自带，Windows不建议，有点麻烦）

CTF比赛中的典型隐写分析工具

- **Binwalk**

- **固件分析工具，常用作路由器逆向、后门分析，或识别二进制图像中的嵌入式文件和可执行代码**

- **命令 ：binwalk 文件名**
- **常用参数：**
- **-e 按照预定义的配置文件来提取(extract.conf)，通常是提取rar**
- **--dd=xxx 提取某种类型的文件，xxx为文件类型(比如--dd=png)**
- **-M 递归提取，需要跟-e或-D配合(比如-Me)**

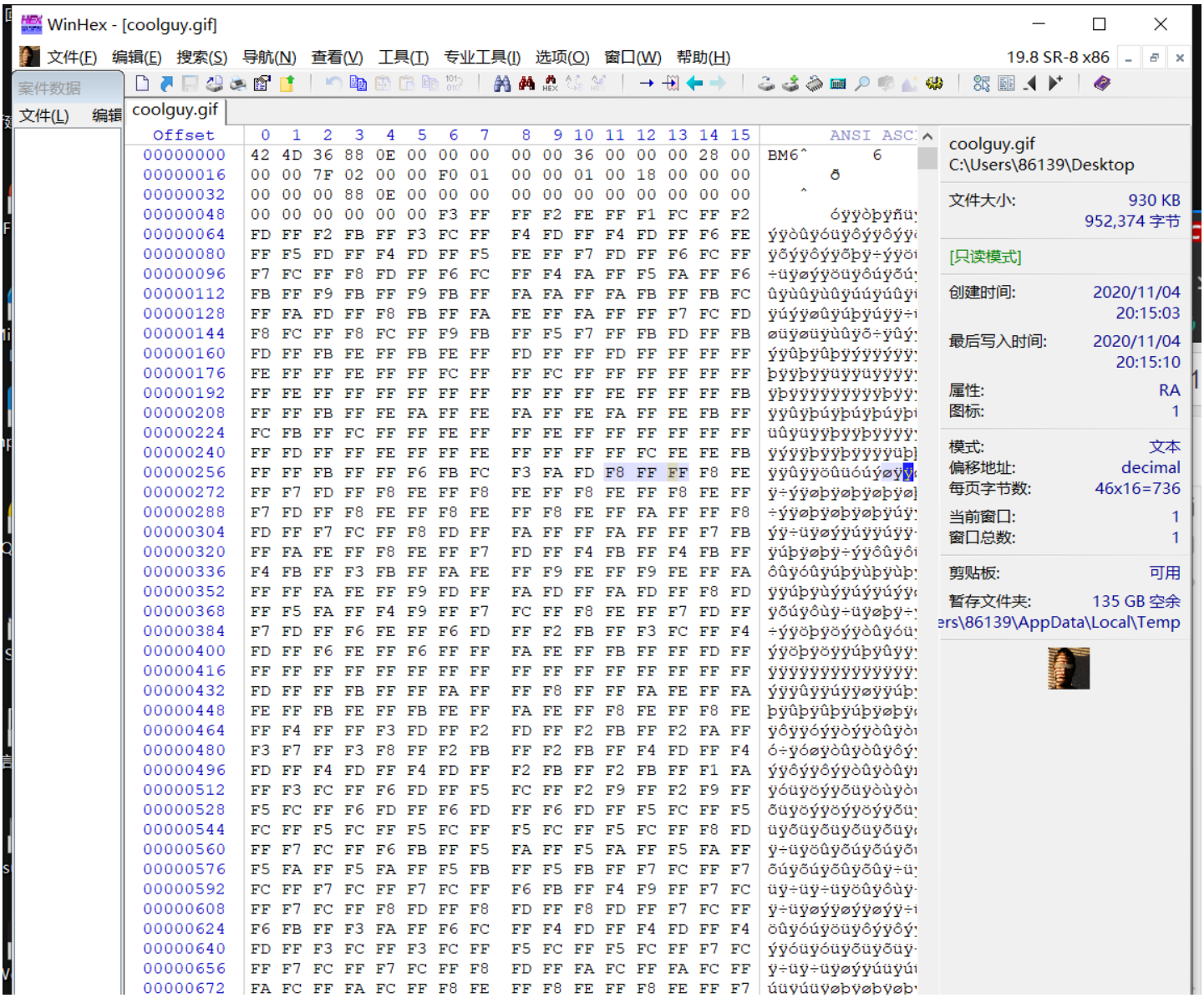


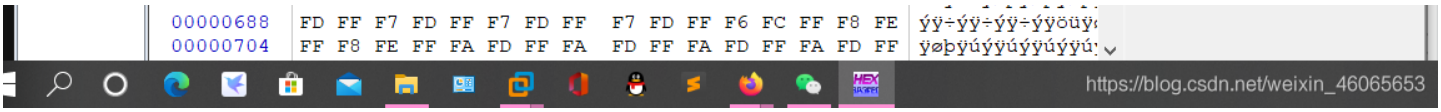
winhex

winhex下载地址

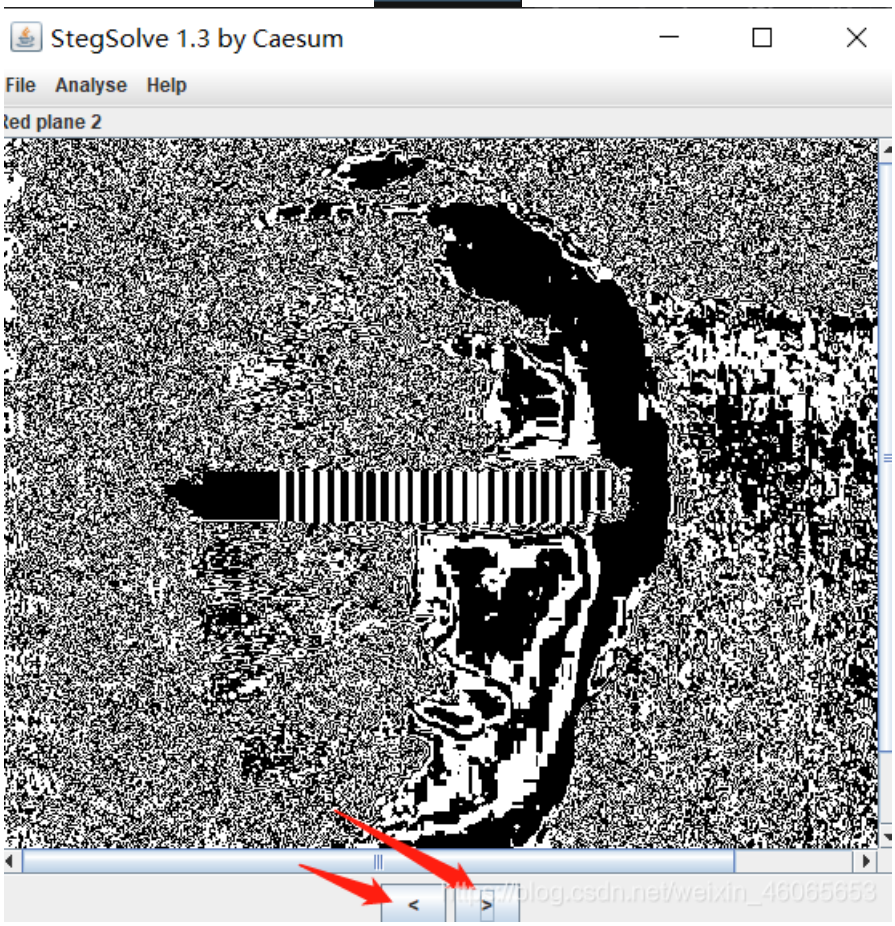
注册码

十六进制文件编译器，常用于检查和修复文件，数据恢复，数字取证等





Stegsolve侧重于图像的图层，色道



CTF比赛中的典型隐写分析工具

- Stegsolve

- 图片通道查看器

Analyse下拉菜单：

File Format：查看文件格式和参数信息，有时候flag会写在图片信息里

Data Extract：数据提取，如LSB隐写等在这个选项中提取信息

Stereogram solver：立体视图，可以左右移动控制偏移量

Frame Broswer：逐帧浏览，如查看快速闪过的GIF图中的flag

Image Combiner：图片结合，可以对两张图片做xor、add、sub等运算

- StegDetect

- 数字图像隐写分析工具，主要针对JPEG

-q：仅显示可能包含隐藏内容的图像

-t：设置要检测哪些隐写算法，支持如下选项：

- -j：检测图像中的信息是否是用jsteg嵌入的。
- -o：检测图像中的信息是否是用outguess嵌入的。
- -p：检测图像中的信息是否是用jphide嵌入的。
- -i：检测图像中的信息是否是用invisible secrets嵌入的。