CTF学习笔记（杂项）

原创

小祥06 已于 2022-04-19 22:18:30 修改 1811 收藏 1
分类专栏： CTF 文章标签： 安全
于 2022-04-12 22:11:24 首次发布

本文链接：https://blog.csdn.net/weixin_51621120/article/details/124134588

CTF的一些简介

网络有：表层网络（触手可及）、深网（需要一定的手段）、暗网（需要专门的工具和技术）三种

白帽子：专门保护信息不被泄露、防御的工程师

黑帽子：专门盗取信息、爆破数据库的人

CTF赛制与题型：Capture The Flag，直译为“夺旗赛”。

CTF题目类型：web安全、逆向工程（Rverse）、漏洞挖掘与漏洞利用（PWN、EXPLOIT）、密码学（Crypto）、调查取证（Misc，又叫杂项）、移动安全（Mobile）

web安全：SQL注入、xss、文件上传、包含漏洞、xxe、ssrf、命令执行、代码审计等。

逆向工程：没有源代码的软件，需要使用工具进行反编译

PWN：二进制破解

刷题平台：

WP网址：

杂项题解题思路：

杂项题目主要可以分为四个方向：文件操作与隐写、图片隐写、压缩文件处理、流量取证技术

1、文件操作与隐写

(1) 文件类型识别：

file命令：适用于不知道后缀名，无法打开文件的情景，当文件没有后缀名或有后缀名而无法正常打开文件时根据识别出的文件类型，通过修改文件后缀名来打开文件。

```
file + 文件名                /*kali系统下使用*/
```

winhex：适用于windows下通过文件头信息判断文件类型，通过winhex程序查看文件头类型，根据文件头类型判断文件类型。

常见的文件头类型如图所示

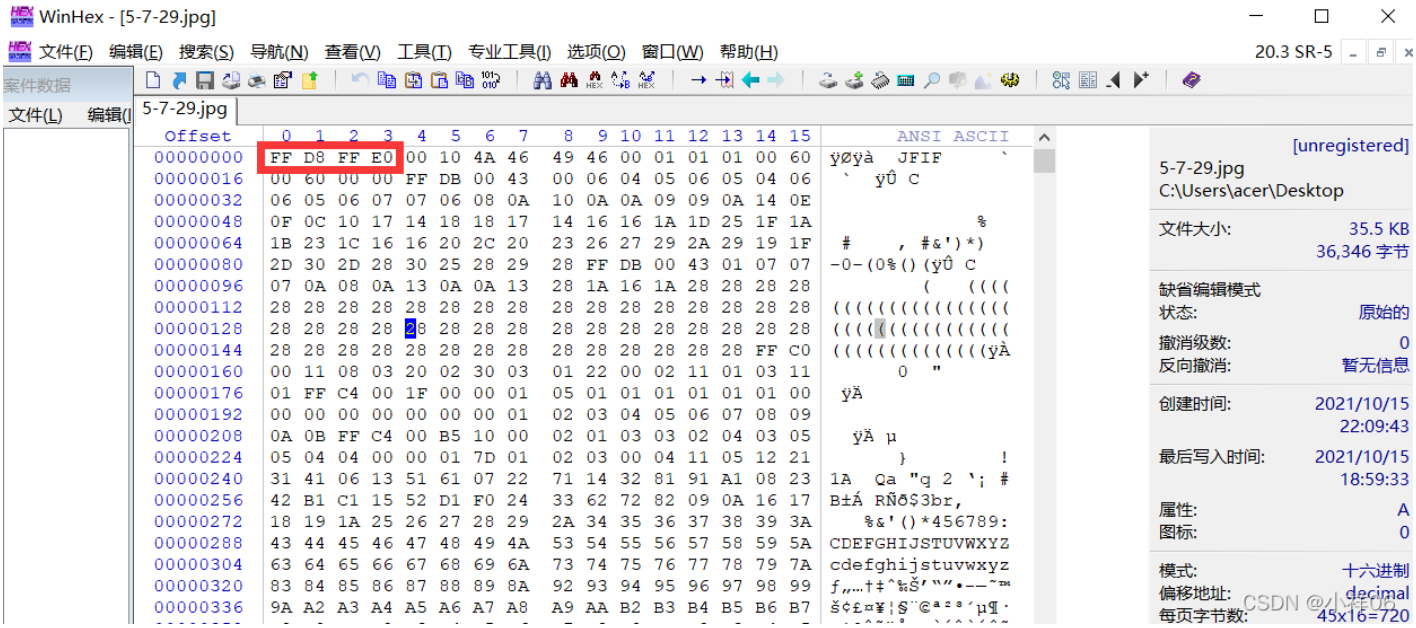
文件类型	文件头
JPEG (jpg)	FFD8FFE1
PNG (png)	89504E47
GIF (gif)	47494638
TIFF (tif)	49492A00
Windows Bitmap (bmp)	424DC001
ZIP Archive (zip)	504B0304
RAR Archive (rar)	52617221
Adobe Photoshop (psd)	38425053
Rich Text Format (rtf)	7B5C727466
XML (xml)	3C3F786D6C
HTML (html)	68746D6C3E
Adobe Acrobat (pdf)	255044462D312E
Wave (wav)	57415645
pcap (pcap)	4D3C2B1A

(2) 使用winhex程序查看文件类型

winhex下载地址：123云盘

https://423down.lanzouo.com/b0f1bltdg

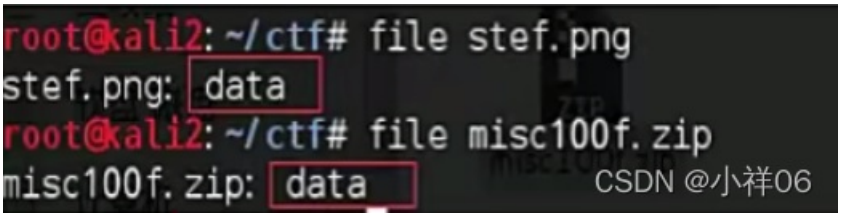
https://pan.baidu.com/s/1Ys6p2u2aHA-BTmuezW0qlw



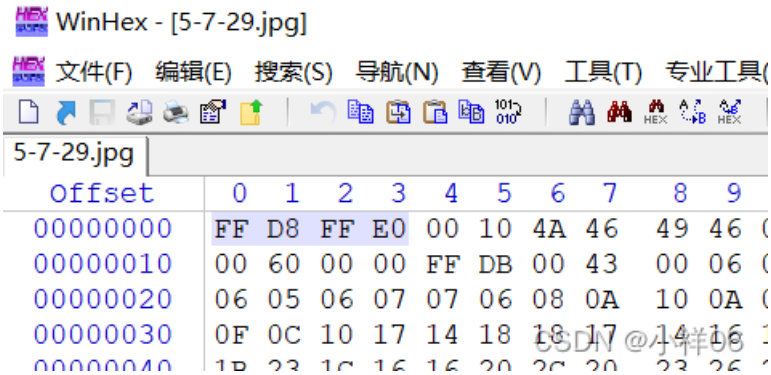
(3) 文件头残缺/错误：适用于文件头部残缺或者文件头部字段错误无法打开正常文件。

文件无法正常打开的情况有两种，一种是文件头部残缺，另一种是文件头部字段错误。正对文件头部残缺的情况，使用winhex程序添加相应的文件头，针对头部字段错误，可以找一个相同文件进行替换。

出现这种情况时，在kali虚拟机下使用file命令，无法显示数据。



对文件进行修复：使用winhex程序打开文件，对文件头进行修改。



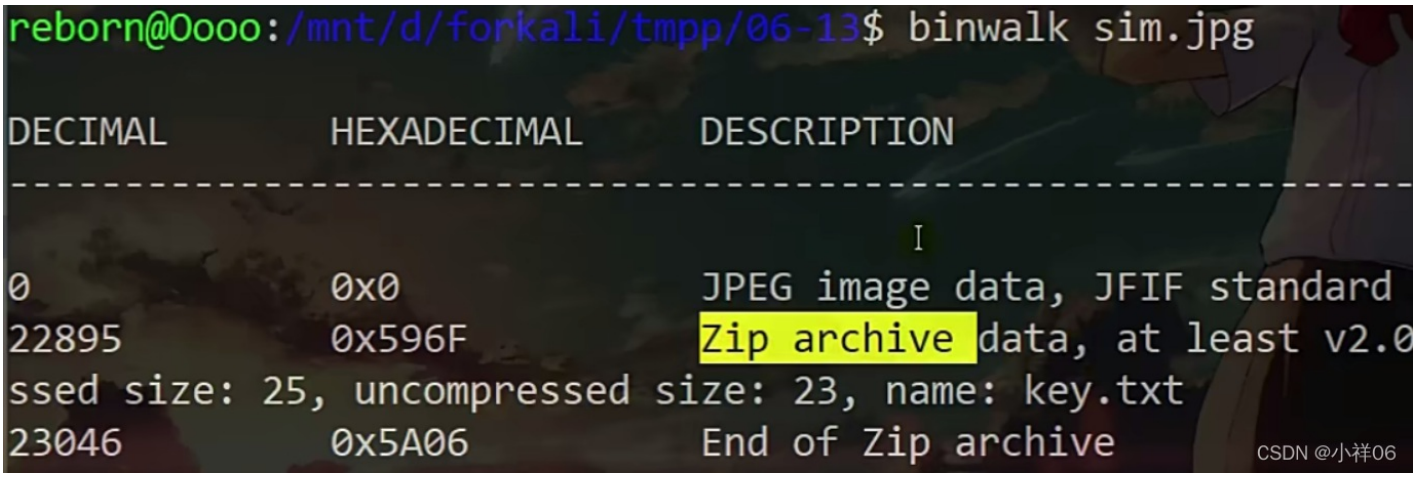
对图片中标注的位置进行修改，可以改变文件头部参数。

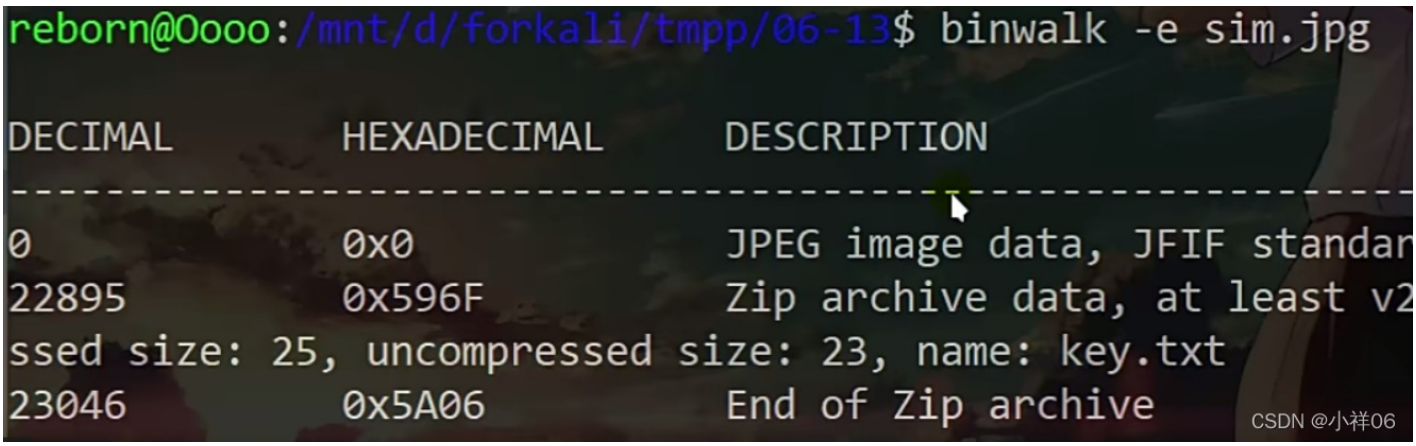
2、文件分离操作

(1) Binwalk工具：

Binwalk是Linux下用来分析和分离文件的工具，可以快速分辨文件是否由多个文件合并而成，并将文件进行分离。如果成功分离会在目标文件的目录。同目录下生成一个形如：文件名_extracted的文件目录，目录中有分离后的文件。用法如下：

```
分析文件：binwalk filename
分离文件：binwalk -e  filename
```



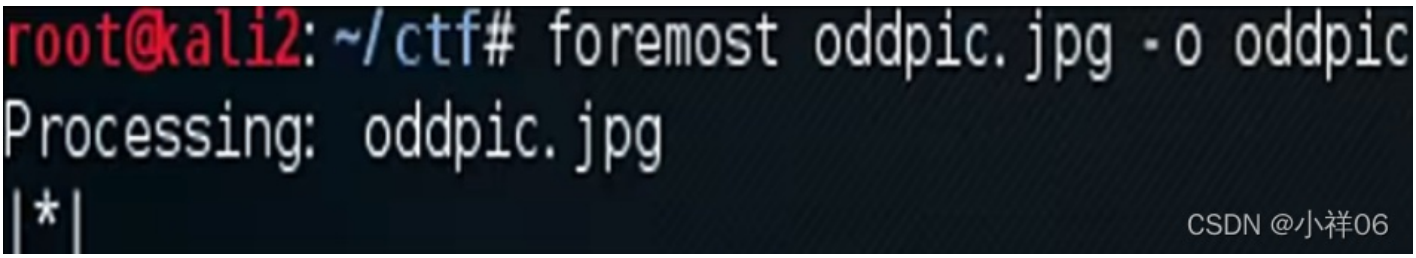


将文件分离之后，会在同级目录下生成一个文件夹，用来存放分离后的文件。binwalk工具在遇到压缩包时，会自动解压。

(2) foremost：

如果binwalk无法正确分离文件，可以使用foremost，将目标文件复制到kali中，成功执行后，会在目标文件的文件目录下生成我们设置的目录，目录中会按文件类型分离文件。foremost命令的用法：

```
foremost 文件名 -o 输出文件名
```



(3) dd命令（相当难用，操作复杂，适用于解决难题）：

当文件自动分离出错或者因为其他原因无法自动分离时，可以使用dd实现文件手动分离。

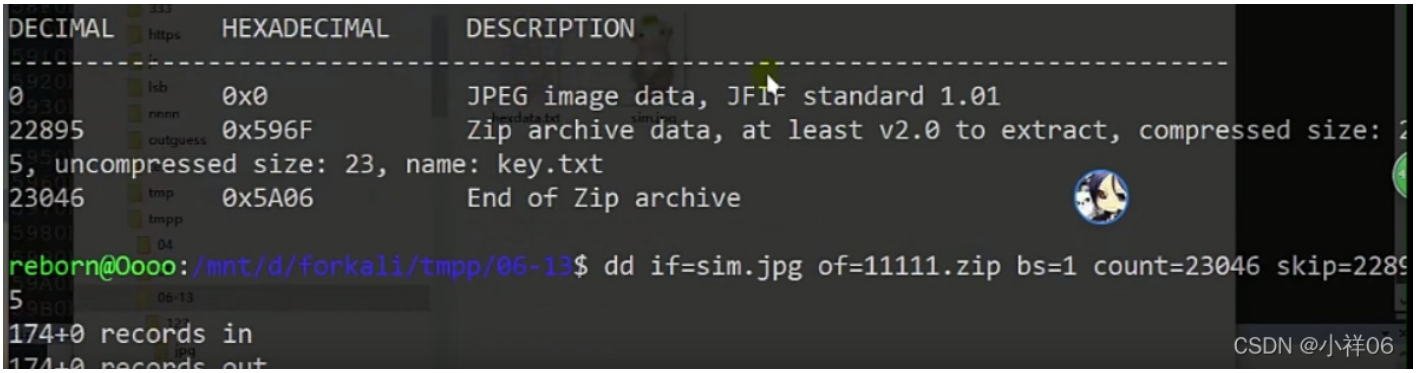
格式：

```
dd if=源文件 of=目标文件名 bs=1 skip=开始分离的字节数
参数说明：
if=file         /*输入文件名，缺省为标准输入*/
of=file         /*输出文件名，缺省为标准输出*/
bs=bytes        /*同时设置读写块的大小为bytes，可以代替ibs和obs*/
skip=blocks     /*从输入文件开头跳过blocks个块后再开始复制*/
```

如下图命令dd if=1.txt of=2.txt bs=5 count=1，输入文件为1.txt，输出文件为2.txt，将bs=5 count=1，将1.txt的前5位取出来形成2.txt文件。

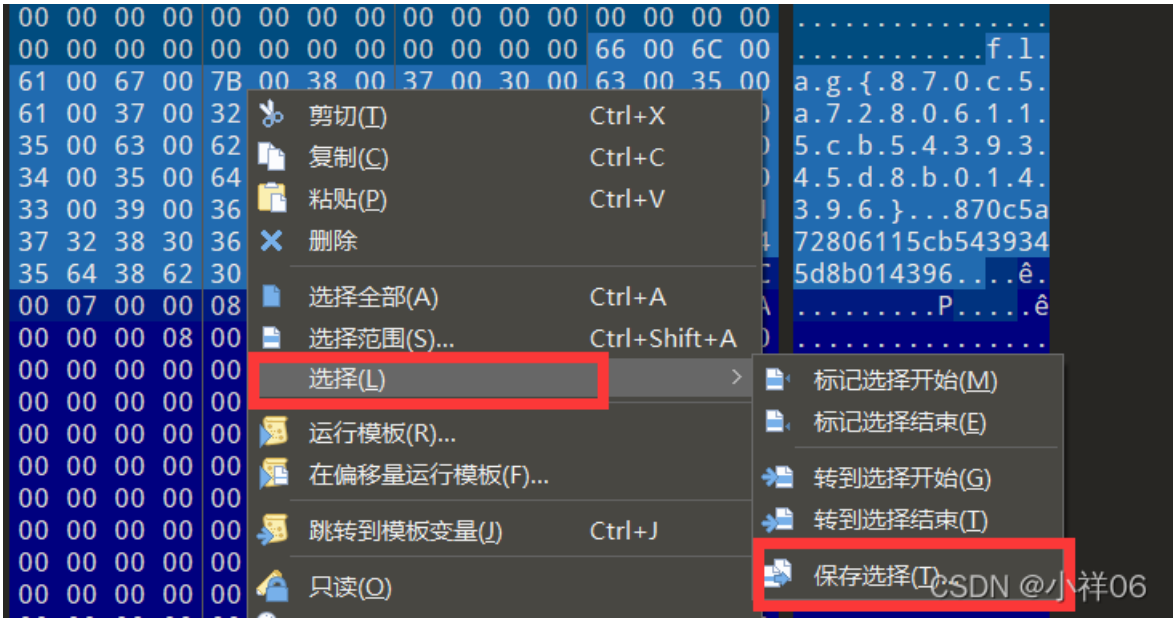
下图命令dd if=1.txt of=3.txt bs=5 count=3 skip=1，输入文件为1.txt，输出文件为3.txt，一个块5个字符，共计3个块，skip=1跳过第一个块。输出文件为后3个块的内容。

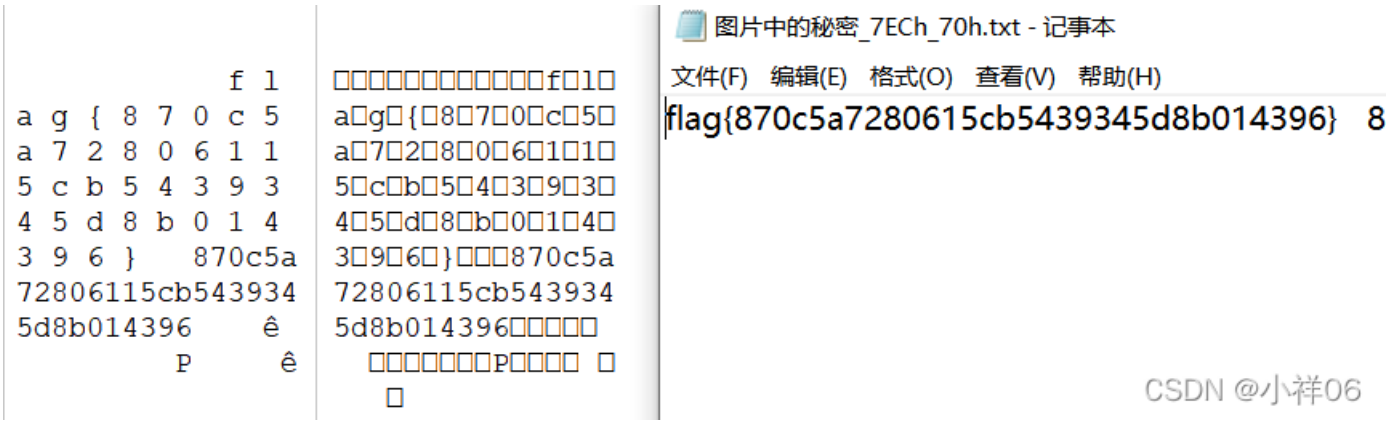
使用binwalk查看文件的组成部分，使用dd命令对文件进行分离，从图中可以看到0-22895是jpeg格式，22896-23046是zip格式，则dd命令格式为：dd if=输入文件 of=输出文件 bs=1 count=23046 skip=22859，即每一块大小为1，跳过前22895块。（一共取23046块，所以count=23046）



使用winhex程序实现文件手动分离，将文件拖入winhex工具，找到要分离的部分，点击复制即可。适用于windows下，利用winhex工具对程序进行手动分离。

步骤如下：选择要分离的部分，选中，右键选择>保存选择，保存成指定格式即可。这样就能将文件中的flag提取出来。





3、文件合并操作

使用md5码检测文件合并的准确性。

(1) Linux下的文件合并：

使用场景：Linux下，通常对文件名相似的文件进行批量合并。格式如下：

```
cat 文件1 文件2>输出文件
```

完整性检测：Linux下计算文件md5：

```
md5sum 文件名
```

(2) Windows下的文件合并：

使用场景：windows下，通常要对文件名相似的文件进行批量合并，格式为：

```
copy /B 合并的文件(文件1+文件2+...+文件n) 输出的文件命令
```

完整性检测：windows下计算md5，格式为：

```
certutil -hashfile 文件名 md5
```

```
D:\CTF\copy>copy /B chapter01+chapter02+chapter03 book
chapter01
chapter02
chapter03
已复制         1 个文件。

D:\CTF\copy>copy /B chapter× book1
chapter01
chapter02
chapter03
已复制         1 个文件。
```



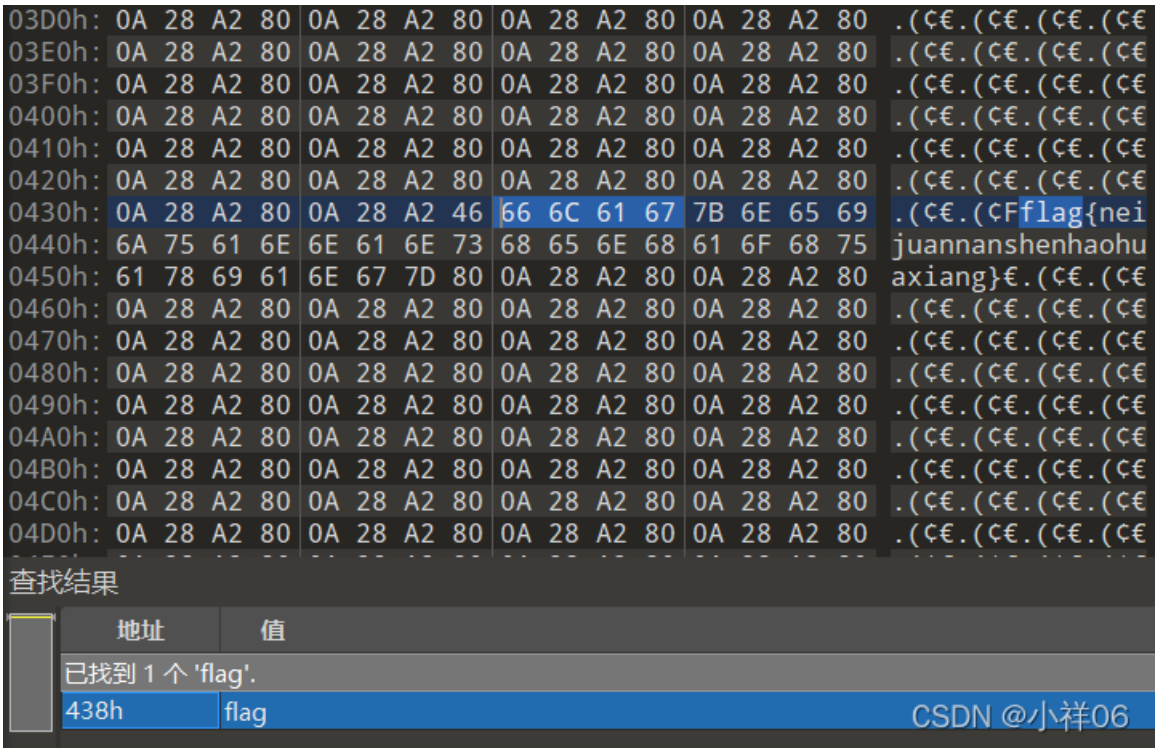
```
reborn@0000 D:\forkali
# certutil -hashfile sim.jpg md5
MD5 的 sim.jpg 哈希:
d09e8a07b6dedb0633aa3c432f931362
CertUtil: -hashfile 命令成功完成。
```


4、文件内容隐写

文件内容隐写，就是直接将Key以十六进制形式写入文件，一般是放在文件的开头或结尾，分析时，**重点观察文件的开头和结尾部分。如果在文件中间部分，通常搜索关键字KEY或flag来查找隐藏内容**。用于Windows下，搜索隐写的文件内容。

(1) Winhex程序/010Editor

将要识别的文件使用Winhex工具进行打开，查找具有关键字或与内容不和谐的部分。



(2) Notepad++工具

使用Notepad++打开文件查看是否具有关键字，安装HEX-Editor后，Notepad++可以实现Winhex的功能。

5、图片隐写

常见的图片隐写：细微的颜色差别、GIF图多帧隐藏（图片通道隐藏、不同帧图信息隐藏、不同帧对比隐写）、Exif信息隐藏、图片修复（图片头修复、图片尾修复、CRC校验修复、长宽高修复）、最低有效位LSB隐写、图片加密（Stegdetect、Outguess、Jphide、F5）

(1) firework

使用Winhex打开文件时，会看到文件头部包含firework 的标识，通过firework可以找到隐藏图片。适用于查看隐写的图片文件。

(2) Exif

Exif按照jpeg的规格在jpeg中插入一些图像/数字相机的信息数据以及缩略图像，可以通过与jpeg兼容的互联网浏览器/图片浏览器/图像处理等一些软件查看Exif格式的图像文件，右键属性，查看文件的详细信息，查看flag信息。