




# 图片隐写工具

原创

匡小萌  于 2020-07-16 22:29:38 发布  2400  收藏 3

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/khy123khy/article/details/107395910>

版权



[CTF 专栏收录该内容](#)

8 篇文章 0 订阅

订阅专栏

## 文章目录

### 图片

[pngcheck](#)

[binwalk](#)

[strings](#)

[winhex 010editor](#)

有用的链接

<http://www.freebuf.com/sectool/94235.html>

<http://ctf.ssleye.com/>

## 图片

[pngcheck](#)

pngcheck.exe在window上，则需要将check的图片放入pngcheck的目录中，才能找到路径。

```
C:\Windows\system32\cmd.exe
E:\CTFtool\misc\pngcheck>pngcheck.exe -v sctf.png
File: sctf.png (1421461 bytes)
 chunk IHDR at offset 0x0000c, length 13
 1000 x 562 image, 32-bit RGB+alpha, non-interlaced
 chunk sRGB at offset 0x00025, length 1
 rendering intent = perceptual
 chunk gAMA at offset 0x00032, length 4: 0.45455
 chunk pHYS at offset 0x00042, length 9: 3780x3780 pixels/meter (96 dpi)
 chunk IDAT at offset 0x00057, length 65445
 zlib: deflated, 32K window, fast compression
 chunk IDAT at offset 0x10008, length 65524
 chunk IDAT at offset 0x20008, length 65524
 chunk IDAT at offset 0x30008, length 65524
 chunk IDAT at offset 0x40008, length 65524
 chunk IDAT at offset 0x50008, length 65524
 chunk IDAT at offset 0x60008, length 65524
 chunk IDAT at offset 0x70008, length 65524
 chunk IDAT at offset 0x80008, length 65524
 chunk IDAT at offset 0x90008, length 65524
 chunk IDAT at offset 0xa0008, length 65524
 chunk IDAT at offset 0xb0008, length 65524
 chunk IDAT at offset 0xc0008, length 65524
 chunk IDAT at offset 0xd0008, length 65524
 chunk IDAT at offset 0xe0008, length 65524
 chunk IDAT at offset 0xf0008, length 65524
 chunk IDAT at offset 0x100008, length 65524
 chunk IDAT at offset 0x110008, length 65524
 chunk IDAT at offset 0x120008, length 65524
 chunk IDAT at offset 0x130008, length 65524
 chunk IDAT at offset 0x140008, length 65524
 chunk IDAT at offset 0x150008, length 45027
 chunk IDAT at offset 0x15aff7, length 138
 chunk IEND at offset 0x15b08d, length 0
No errors detected in sctf.png (28 chunks, 36.8% compression).
```

<https://blog.csdn.net/khy123khy>

运行命令 `pngcheck.exe -v xx.png`，可以详细查看每个数据块的情况

-7 打印文本块的内容，除了多于128个的字符，因为只有7位。

-f 即使在出现重大错误后仍强制继续。

-p 显示PLTE, tRNS, hIST, sPLT和PPLT的内容（可与-q一起使用）。

-q 安静地测试（仅输出错误）。

-s 在另一个文件中搜索PNG。

-t 显示tEXt块的内容（可与-q一起使用）。

-v test verbosely（打印大多数块数据）。

-x 搜索PNG并在找到时提取它们。

## binwalk

binwalk在kali里面自带此工具，在ubuntu16.04需要apt-get install，

直接通过命令 `binwalk xx.xx` 来查看详细数据，比如可以发现在其中隐藏的另一张图片或者压缩包，这是通过分析文件头来进行识别。`binwalk -e xx.xx` 可以提取已知文件类型。详解参数直接 `binwalk` 可以查看所有的参数设置。

### ##foremost

文件分离的工具，也是Kali自带的，不仅仅局限于图片中，流量包也可以提取。当binwalk提取不好使可以用foremost试试，cd入当前文件目录，`foremost xxx.xx`

`http://zjw.dropsec.xyz/uncategorized/2016/08/18/CTF%E4%B8%AD%E5%B8%B8%E8%A7%81%E5%9B%BE%E7%89%87%E9%9A%90%E5%86%99.html`

foremost -t 可以修复损坏的文件

### ##file

file命令用于来探测指定文件的文件类型，

-b: 列出辨识结果时，不显示文件名称；

-c: 详细显示指令执行过程，便于排错或分析程序执行的情形；

-f<名称文件>: 指定名称文件，其内容有一个或多个文件名称时，让file依序辨识这些文件，格式为每列一个文件名称；

-L: 直接显示符号连接所指向的文件类别；

-m<魔法数字文件>: 指定魔法数字文件；

-v: 显示版本信息；

-z: 尝试去解读压缩文件的内容。

## strings

strings命令在对象文件或二进制文件中查询可打印字符串，字符串是4个或更多可打印字符的任意序列，以换行符或空字符结束

## 01 strings命令语法

```
strings [ -a ] [ - ] [ -o ] [ -t Format ] [ -n Number ] [ -Number ] [ file ... ]
```

## 02 strings命令选项

```
-a 或 -          搜索整个文件，而不仅仅是数据段，以寻找可显示的字符串。如果省略这个标志，那么 strings 命令只在对象文件的初始
-n Number       指定最小的字符串长度（除了缺省的 4 个字符以外）。字符串长度的最大值是 4096。这个标志与 -Number 标志相同
-o             列出文件中每个跟随在其八进制偏移量之后的字符串。这个标志与 -t o 标志相同。
-t Format      列出从文件最开始起，每个跟随在其偏移量之后的字符串。该格式取决于用作 Format 变量的字符。
    - d
    - 以十进制写下偏移量。
    - o
    - 以八进制写下偏移量。
    - x
    - 以十六进制写下偏移量。
    注：当 -o 和 -t Format 标志在一个命令行上多次定义，那么最后指定的标志控制 strings 命令的行为。
-Number       指定最小的字符串长度（除了缺省的 4 个字符以外）。字符串长度的最大值是 4096。这个标志与 -n Number 标志相同
File          要搜索的二进制文件或对象文件。
```

<https://blog.csdn.net/khy123khy>

## winhex 010editor

这两个都是十六进制文件查看器。