

入门知识

前言

STEGA即隐写术，将信息隐藏在多种载体中，如：视频、硬盘和图像，将需要隐藏的信息通过特殊的方式嵌入到载体中，而又不损害载体原来信息的表达。旨在保护需要隐藏的信息不被他人识别。信息隐蔽技术有：1) 隐写术、2) 数字水印、3) 隐蔽信道、4) 阙下信道、5) 匿名信道。

这一章主要讲图片隐写。

CTF隐写术现状

CTF比赛中的隐写术现状

- 隐写套路较为固定
- 比赛工具较为成熟

好处：通常题目难度较低，即使没有解题思路，依次尝试各个解法往往也能在没发现提示的情况下找出问题所在。

坏处：容易形成思维定势，一旦题目考察方式不常规，往往容易无从下手，不知道从哪开始去分析，失去独立发现问题和思考的能力。

拿到图片


- Binwalk+winhex方向
- StegSolve方向
- StegDetect方向

LSB隐写介绍

一种最简单的图片隐写术就是在一个纯色背景中用十分相近（人肉眼无法立即识别出来）的颜色写入信息。

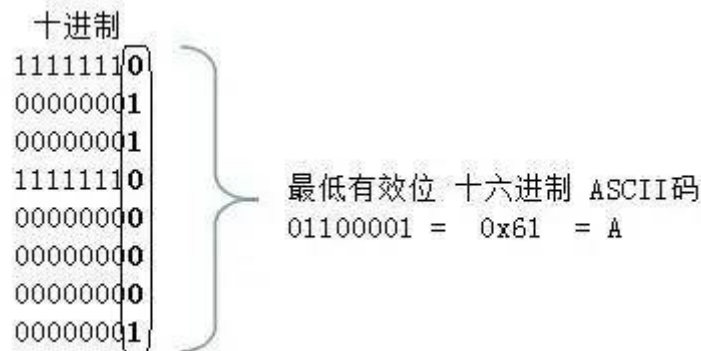
另一种常见的方式是利用LSB来进行隐写，LSB也就是最低有效位 (Least Significant Bit)。原理就是图片中的像素一般是由三种颜色组成，即三原色，由这三种原色可以组成其他各种颜色，例如在PNG图片的储存中，每个颜色会有8bit，LSB隐写就是修改了像素中的最低的1bit，在人眼看来是看不出来区别的，也把信息隐藏起来了。譬如我们想把'A'隐藏进来的话，如下图，就可以把A转成16进制的0x61再转成二进制的01100001，再修改为红色通道的最低位为这些二进制串。

颜色	二进制	十进制	
红	11111110	254	}
绿	00000000	0	
蓝	00000000	0	



红

红色通道最后一位被修改：



每个通道都修改最后一位，修改8次就能隐藏一个ASCII码

如果是要寻找这种LSB隐藏痕迹的话，Stegsolve是个神器，可以用来辅助我们进行分析。

注：jpg是有损压缩，无法LSB隐藏信息；png虽有压缩却是无损的，bmp没有被压缩，这两者都可用LSB隐藏信息。

图片宽高

PNG文件中，每个数据块都由四个部分组成，如下：

- 长度(Length)：指定数据块中数据区域的长度，长度不可超过 $(2^{31}-1)$ 个字节
- 数据块类型码(Chunk Type Code)：数据块类型码由ASCII字母(A-Z和a-z)组成的"数据块符号"
- 数据块数据(Chunk Data)：存储数据块类型码指定的数据
- 循环冗余检测(CRC)：存储用来检测是否文件传输有误的循环冗余码

shack.png

文件头 长度 数据块类型码

Offset 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 19 48 44 52 PENG IHDR

00000016 00 00 01 C9 00 00 00 EE 08 06 00 00 00 BE 91 75

00000032 39 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 9 sRGB 0i é

00000048 20 00 49 44 41 54 18 5E 8C BD C9 8F AC 59 92 DD IDATx^G4E -Y'Y

00000064 77 7D F6 F0 18 DF 18 43 65 75 75 55 B1 9B CD 05 w!00 B^CeuuU±i

00000080 21 B2 F9 5F 6A A1 A5 96 5A 08 02 B4 10 A4 0D 85 !^ù_j;¥~Z ' M ...

00000096 26 55 EC 6E 0A 22 20 46 90 08 91 14 AB BB 58 4D 6Uln " @ ' «»XM

00000112 B2 C6 CC 7C F9 C6 98 C3 67 17 7E E7 98 DD EF BA ^IjùE^Ag ~q^Yi

00000128 47 64 81 5E C8 8A 78 1E EE DF 70 BF 7B ED 98 1D Gd ^EŠx iBpç(i~

00000144 3B 66 B7 F7 5F FF 4F FF EB AE D7 EB 95 5E 29 A5 ;f~÷ yOyè«xè^)^¥

00000160 D7 DB 15 7E 1F EC B6 65 B8 DB 94 5E BF 5F 06 FD xÜ ~ iqe,Ü^~^è_ y

00000176 41 19 0E 07 A5 DF EF EB 6F BB 5D 29 DB ED A6 6C A ¥šieow}}Üi;l

00000192 B7 DB B2 DB ED 4A AF F4 CB 70 38 E4 CB 65 B3 D9 -Ü=ÜiJ^öEp8aEe^Ü

00000208 14 8E D4 1F F4 4B D9 71 C0 52 06 83 81 3E B7 5A ŽÖ öKÜqÀR f > >Z

00000224 AF CB AA 14 FD CE 77 F9 8F 57 FE E4 FC 7E F1 A5 -E^ yîwù Wpâü~ñ¥

00000240 61 E9 EB BF 81 AE AB FE A5 D7 AB 9F EF 7A F8 7B aéeèç 0«p¥««Yçzø{

00000256 D9 F9 5C 9C 4E 17 C7 11 B8 D6 E6 7B 3E EA B6 F4 Üù\«N Ç ,Ç«{>èqó

00000272 CB AA 0C 86 43 DD 4B BF D7 D7 27 76 F5 CB 3E 35 È^ tCÝKçx~^vóÈ>5

00000288 D7 37 2C A5 F0 57 7E CF FF FA DC 7B 29 BA 47 DD x7,¥øW~îyúÜ{)°GÝ

00000304 C3 66 5B 16 EB 65 B9 DD 2C 7D 7E 3E EB AB D0 8B Äf[èe^Y, }~>è«B<

00000320 E3 EB 73 BB 6D 19 0D 47 E5 68 34 28 C3 9E 8F E7 äesxm Gâh4(Äž ç

00000336 4B 8D 9F DB 9D 6F B9 3F 28 A3 F1 A8 8C 86 C3 32 K YÜ o^? (Äñ^G+Ä2

00000352 5E EE 4A 8F B7 EB 4D EC CA 46 63 EE FF 78 BF DF ^iÜ -èMièFciyxçB

00000368 F7 33 D1 75 6D 77 A5 DF 2B 65 BB 59 97 D5 7A 59 ÷3Ñumw¥B+e»Y~ÖzY

00000384 CA 66 5B 76 DB 4D 19 8F 86 65 38 E8 97 E5 62 51 Èf{vÜM te8è~âbQ

00000400 D6 9B 75 59 AF 57 7A 1E AB D5 BA 1C 1D 4D CB F3 Ç»uY^Wz «Ö° MÈó

00000416 E7 CF CB DD DD 7D B9 BB BB D5 F5 AC D7 EB B2 5E çIÈYÝ}»»Öö~«è^

00000432 2D CB 6E BB 2C 0F F7 F7 3A FE 64 32 F1 98 F6 7A -En», ++:pd2ñ^öz

00000448 FA FB 68 34 2A BF F9 CD 6F CA FD FD 7D F9 C9 1F úùh4*èùioEýýçüÈ

00000464 FF B4 1C CF 4E CB 60 D0 2F E3 F1 58 7F 7F 78 78 y^ INÈ^D/âñX xx

00000480 28 1F 3F 7E 2C 5F 7F F3 4D B9 BB BD D5 39 78 1E (?~, _ öM^»«ö9x

00000496 D3 C9 A4 4C A6 D3 72 75 75 A5 F7 F9 EC 6A B5 2A ÔÈ«L!Öruu¥~ùijp*

00000512 A3 D1 58 F7 C6 79 06 FD 7E F9 74 75 55 4A 7F A0 èNX÷Ey ý~ùtuÜJ

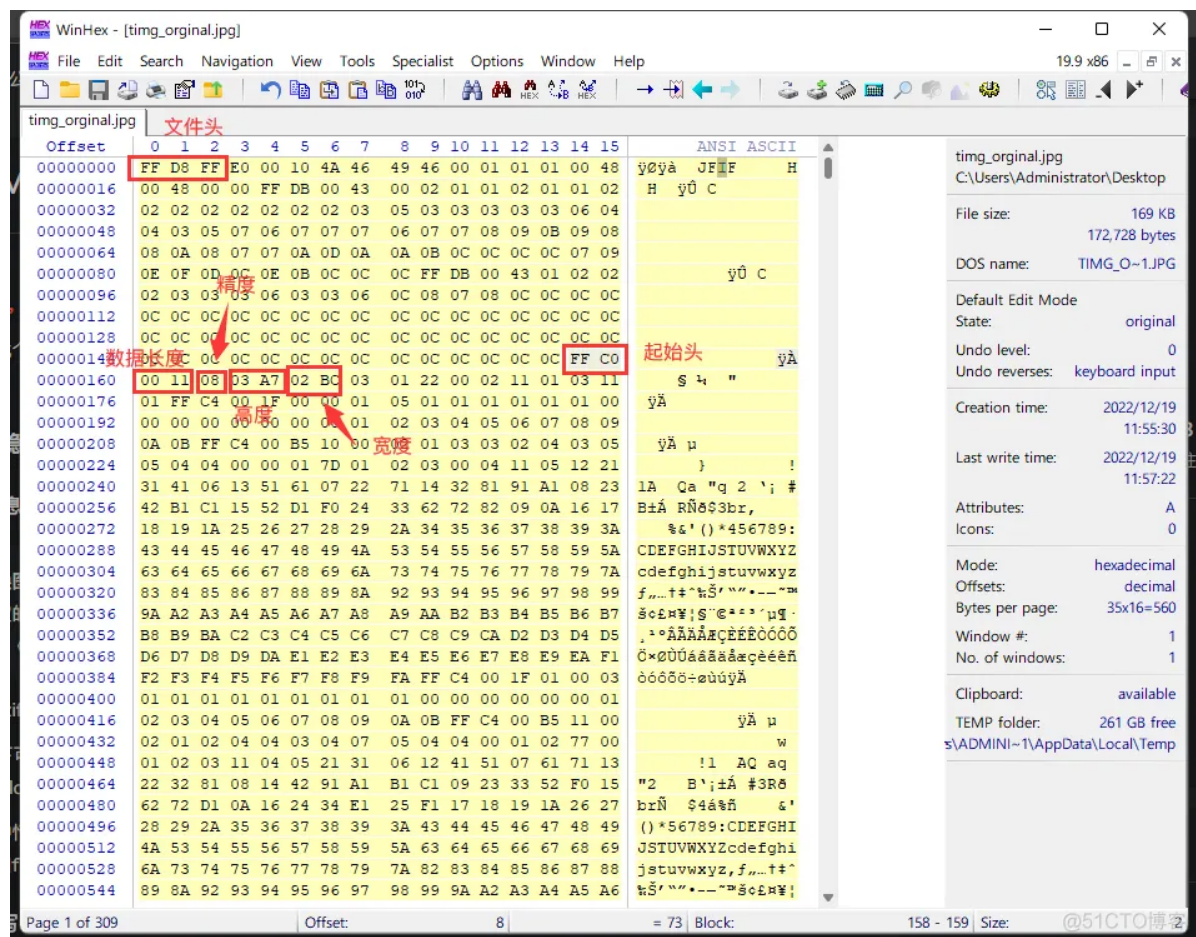
00000528 E7 CC B5 2E 16 0B 1D 6F 3A 9D 96 E5 72 A9 FB 3F çIu. o: -Äxèù?

00000544 3F BF D0 BF F9 0C C7 E1 FD E9 74 52 A6 D3 23 8D ?èBçù ÇéýéçR!Ö#

shack.png C:\Users\Administrator\Desktop
File size: 10.0 MB
10,500,343 bytes
Default Edit Mode: original
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 2022/12/16 12:34:28
Last write time: 2022/12/16 11:44:00
Attributes: A
Icons: 0
Mode: hexadecimal
Offsets: decimal
Bytes per page: 35x16=560
Window #: 1
No. of windows: 1
Clipboard: available
TEMP folder: 260 GB free
s\ADMINI~1\AppData\Local\Temp

Page 1 of 18,751 Offset: 0 = 137 Block: n/a Size: @51CTO

JPG图片的头数据为 FF D8 FF，其他重要信息如图所示。



因此有时可以通过把一张完整的图片通过手动修改图片高度来隐藏图片下面一部分内容。

EXIF信息

在我们拍摄图片时，exif可以记录数码照片的属性信息和拍摄数据。

右击图片，点击熟悉，选择详细信息，这里面可以看到图片拍摄的一些值，有时候还能找到经纬度。



在kali里，我们可以用exiftool工具来查看更详细的exif数据。

```
exiftool cat.jpg
```

常用工具

- Stegsolve
- QR Reader
- convert
- Adobe Photoshop
- 010 Editor
- WinHex
- binwalk

实战案例

[CTF Misc\(1\)图片隐写基础以及原理，覆盖了大部分题型51CTO博客ctf 图片隐写](#)

参考资料

CTFer成长之路-Nu1L战队-Misc部分