链滴

隐写术——计算机中数据隐藏的艺术

作者：YYJeffrey
原文链接：https://ld246.com/article/1661160636595
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/bing/20191206.jpg?imageView2/1/w/960/h/540/interlace/1/q/100">
<img src="https://ld246.com/images/img-loading.svg" alt="dog.png" data-src="https://
3logfile.com/file/2022/08/dog-16c108ea.png?imageView2/2/interlace/1/format/jpg">
当你看到上面这张图片时，你认为这是一张普通不过的图片。你使用肉眼读出了图片本身的信息
但诚然，它还隐藏着你看不到的信息。
将该图片使用 StegSolve 打开，将红绿蓝任一通道调整至 0 时，惊奇的一幕出现了，图片左上
多了一个二维码。
<img src="https://ld246.com/images/img-loading.svg" alt="202208221403.gif" data-src
"https://b3logfile.com/file/2022/08/202208221403-83acf90d.gif">
使用微信或其他扫码工具查看得到了如下内容。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2022/08/image-177b951b.png?imageView2/2/interlace/1/format/jpg"><
p>
其实该图片是通过将原图像素值的 n 个最低有效位替换为与二维码图片像素值相同数量的最高有
位所得到的。该方法也称为 LSB 隐写（最低有效位隐写），该兴趣的朋友可以
行科普这方面的具体知识。
<hr>
1050.wav
当你听到上面这段音频时，你认为这只是一段普通不过的曲子。仅凭耳朵你只能听到声音表面的
息，其实它的信息远不止这些。
将该音频拖入 SilentEye 中，使用 Decode 尝试解码，我们得到了一串由 1、0 和\组成的字符
。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2022/08/image-5e578614.png?imageView2/2/interlace/1/format/jpg"></
>
显然这串字符串还有更深层的含义。正当你没了头绪的时候，突然想到了可以用“—”代表 1，“
”代表 0，这样就组成了一串 摩斯电码。
转换之如下所示：
<pre><code class="highlight-chroma"><span class="highlight
cl">---.-.--.-.----/---..-.--....-./--..--....-----/--..---...-----/-.-.--.--.--.--/-..----.--...../--....---....-./---.--.-.
..-..
</code></pre>
此时使用在线摩斯电码转换器或其他工具，你惊奇地还原出了一句地球人都懂的暗语。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2022/08/image-72304908.png?imageView2/2/interlace/1/format/jpg"></
>
上述隐藏数据的方法原理类似于图片的 LSB 隐写。当然，音频还能通过波形来隐藏数据，但或
听着会有些刺耳。音频 + 摩斯码的组合也曾被用于谍战中。
<hr>
info.zip
当你打开上面的这个压缩包时，你变得比先前更为谨慎，虽然其中只有一个文档，但你却仔细观
文档的每一个角落，生怕会错过任何重要的信息。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2022/08/image-5a2e498b.png?imageView2/2/interlace/1/format/jpg"></
>
文中只有一行字，但你 Ctrl+A 全选文档后，似乎在中间选中了什么，恭喜你发现了信息之外的
息，这是一行隐藏的文字。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2022/08/image-19f21d36.png?imageView2/2/interlace/1/format/jpg"></
>
通过打开 Word 选项并勾选“隐藏文字”后，方可查看到被隐藏的信息。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:
/b3logfile.com/file/2022/08/image-11925bc9.png?imageView2/2/interlace/1/format/jpg"></

>
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:/b3logfile.com/file/2022/08/image-dd3d0796.png?imageView2/2/interlace/1/format/jpg">
但这真的就结束了吗？
显然没有这么简单，问题并不出在这个文档上，而是蕴藏在这个压缩包上。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:/b3logfile.com/file/2022/08/image-c06a2f9f.png?imageView2/2/interlace/1/format/jpg"></>
将其拖进 winhex 查看其十六进制，可以看到底部有一部分数据较其他数据完全不同，它十分的整有序。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:/b3logfile.com/file/2022/08/image-e744902b.png?imageView2/2/interlace/1/format/jpg"></>
这里不卖关子了，其实这是一串通过 Base64 加密的字符串，通过在线的密软件即可获得最终的信息。
<img src="https://ld246.com/images/img-loading.svg" alt="image.png" data-src="https:/b3logfile.com/file/2022/08/image-29977da1.png?imageView2/2/interlace/1/format/jpg"></>
上述数据隐藏的方法是通过将两个文件合并到达的，你也可以通过文件分离工具将其分离。
<hr>
本文只是浅显的讲述了隐写术的奥秘，除了上面所提到的数据隐写的方法，还有数不胜数的方法
如果你也和博主一样对隐写术感兴趣的话，推荐学习和阅读书籍 《数据隐藏技术揭秘，如果你想进一步学习隐写术，你可以通过练习 CTF 杂项，解出难后你一定会惊呼玄妙。
文章编写与素材制作不易，忘转载时附上文章来源，谢谢！