CTF Misc常用工具(二)

原创

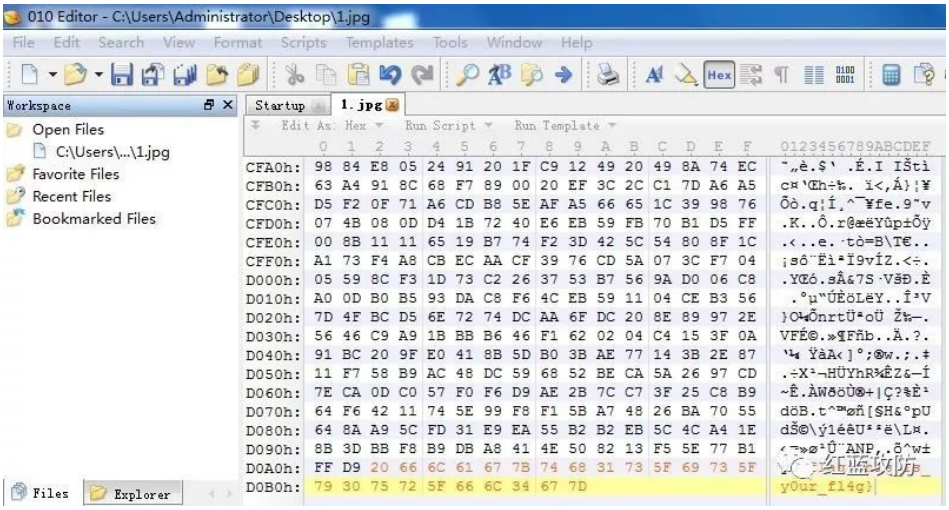
Cer0 于 2019-10-18 21:26:57 发布 1839 收藏 20
分类专栏： CTF 文章标签： Misc

本文链接：https://blog.csdn.net/chenl_ce2009/article/details/102632353

010 editor

010 Editor是一款专业的文本编辑器和十六进制编辑器，它可以编辑文本文件，包括 Unicode 文件、批处理文件、C/C++、XML 等，功能全面且强大，常用于CTF题目中查看图片等文件的十六进内容查看、修改、搜索等。

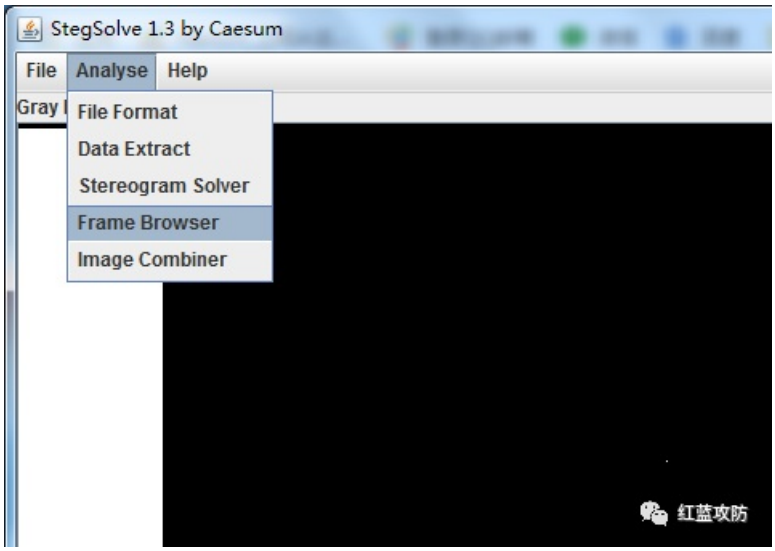
用010editor打开文件既可以常文件的十六进制内容，也可以修改或者查查看正常文件之外的内容。(例如，正常jpg文件是以FF D8开头，FF D9结束，下图文件末尾被增加了额外内容flag)



同样功能的软件还有winhex等。

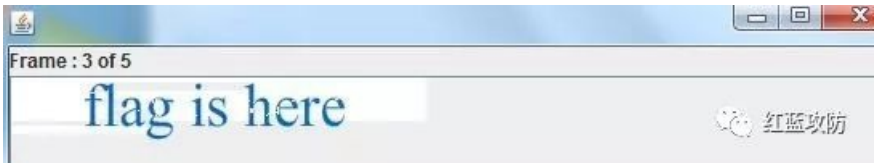
stegsolve

CTF中图片隐写常用工具，可以查看图片每一帧，可对图片进行合并等操作。



查看动态图片的每一帧，如test.gif是一个动态图，想看清楚每一帧的图片内容，可通过stegsolve实现。

查看每一帧图片：



即可得到GIF图片里面的flag。(题目来源：http://119.23.73.3:6001/misc2/flag.png)

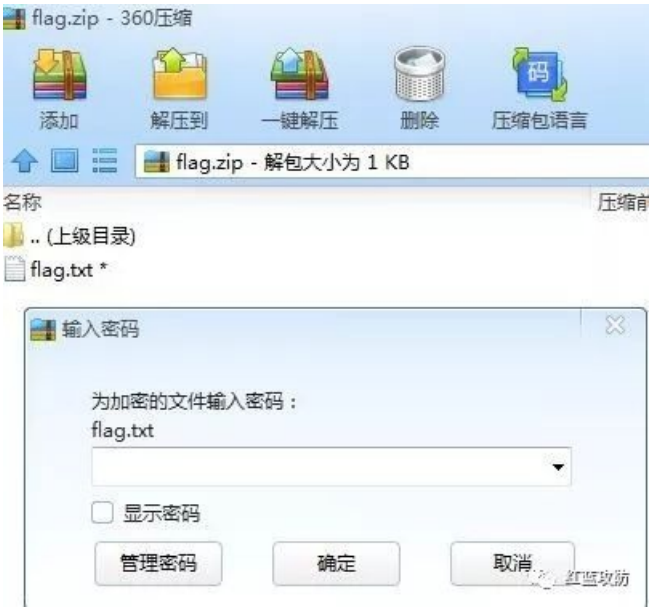
ZipCenOp.jar

zip伪加密题目解密工具，zip伪加密形成的原因是，修改正常zip文件头的加密标志位。(可参考文章：https://blog.csdn.net/kajweb/article/details/76474476)

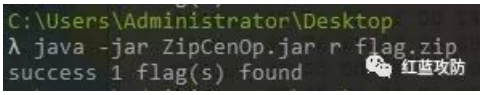
工具使用方法：

```
java -jar ZipCenOp.jar e xxx.zip #加密
java -jar ZipCenOp.jar r xxx.zip #解密
```

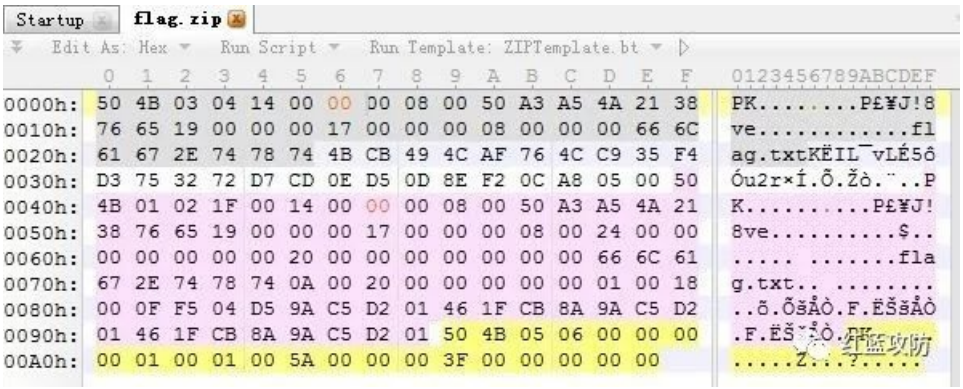
一道来自bugku的题目：



打开文件需要密码，根据题目提示：zip伪加密，使用ZipCenOp.jar进行解密：



或者，使用010 editor修改头文件加密标志位：



不足之处请留言反馈，谢谢！