

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](#)

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/chen_ce2009/article/details/102632353

版权



[CTF 专栏收录该内容](#)

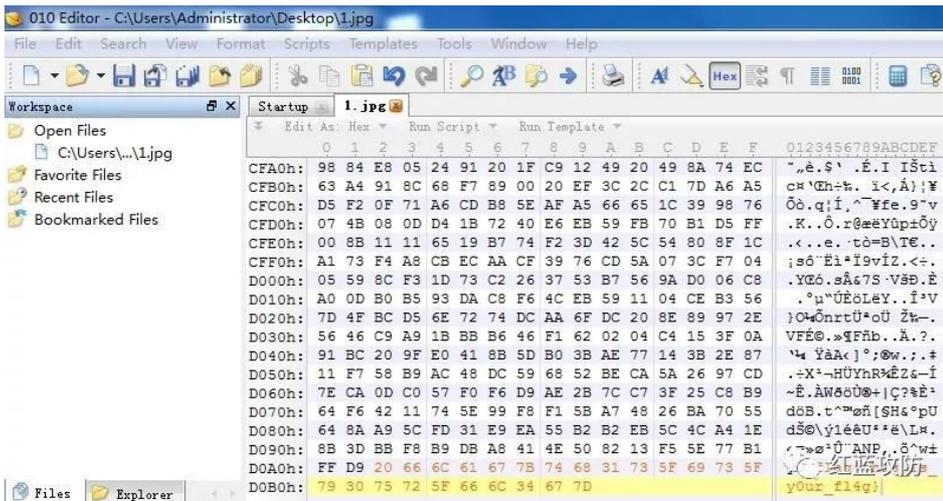
5 篇文章 0 订阅

订阅专栏

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。

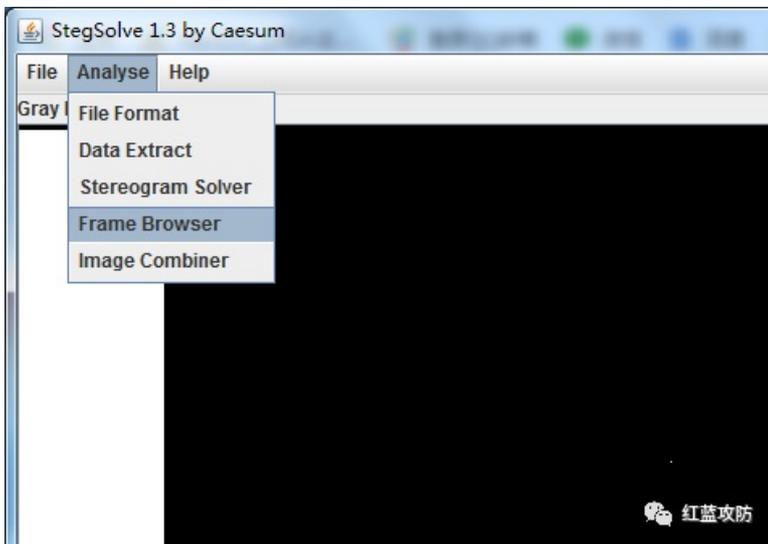
用010editor打开文件既可以常文件的十六进制内容, 也可以修改或者查查看正常文件之外的内容。(例如, 正常jpg文件是以FF D8开头, FF D9结束, 下图文件末尾被增加了额外内容flag)



同样功能的软件还有winhex等。

stegsolve

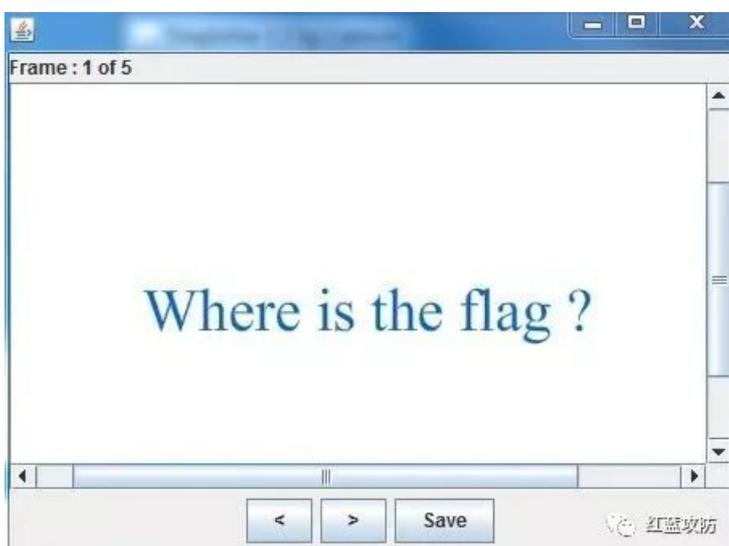
CTF中图片隐写常用工具, 可以查看图片每一帧, 可对图片进行合并等操作。

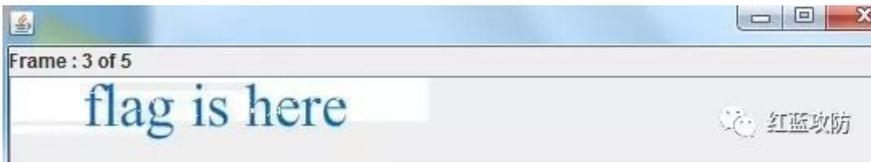


查看动态图片的每一帧，如test.gif是一个动态图，想看清楚每一帧的图片内容，可通过stegsolve实现。

Where is the flag ?

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：

```
C:\Users\Administrator\Desktop
λ java -jar ZipCenOp.jar r flag.zip
success 1 flag(s) found
```

或者，使用010 editor修改头文件加密标志位：

```

Startup flag.zip
Edit As: Hex Run Script Run Template: ZIPTemplate.bt
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 50 4B 03 04 14 00 00 00 08 00 50 A3 A5 4A 21 38 PK.....P£¥J!8
0010h: 76 65 19 00 00 00 17 00 00 00 08 00 00 00 66 6C ve.....fl
0020h: 61 67 2E 74 78 74 4B CB 49 4C AF 76 4C C9 35 F4 ag.txtKĒIL~vLÉ5ó
0030h: D3 75 32 72 D7 CD 0E D5 0D 8E F2 0C A8 05 00 50 Óu2r×Í.Ö.Žó.~...P
0040h: 4B 01 02 1F 00 14 00 00 00 08 00 50 A3 A5 4A 21 K.....P£¥J!
0050h: 38 76 65 19 00 00 00 17 00 00 00 08 00 24 00 00 8ve.....$.
0060h: 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6C 61 .....fla
0070h: 67 2E 74 78 74 0A 00 20 00 00 00 00 00 01 00 18 g.txt.....
0080h: 00 0F F5 04 D5 9A C5 D2 01 46 1F CB 8A 9A C5 D2 ..š.ÖšÄÖ.F.ĚššÄÖ
0090h: 01 46 1F CB 8A 9A C5 D2 01 50 4B 05 06 00 00 00 .F.ĚššÄÖ.££ššÄÖ
00A0h: 00 01 00 01 00 5A 00 00 00 3F 00 00 00 00 00 00 .....Z.....

```

flag.zip - 解包大小为 1 KB

名称	压缩前	压缩后	类型
.. (上级目录)			文件夹
flag.txt	1 KB	1 KB	文本文档

```

flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag {Adm1N-B2G-kU-SZIP}

```

不足之处请留言反馈，谢谢！