

实验吧隐写术WP(五)

原创

Neil-Yale 于 2017-04-02 13:32:06 发布 4172 收藏

文章标签: [wp x CTF c#系统附数据库](#)

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。

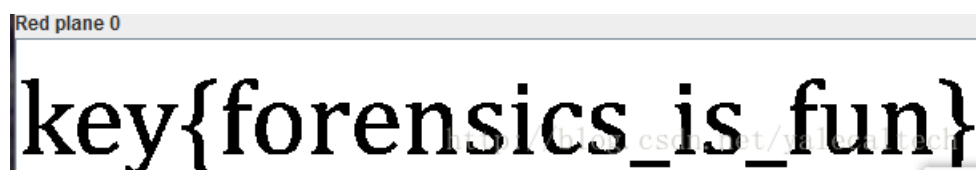
本文链接: <https://blog.csdn.net/yalecaltech/article/details/68951789>

版权

1.so beautiful so white(<http://www.shiyanbar.com/ctf/1904>)

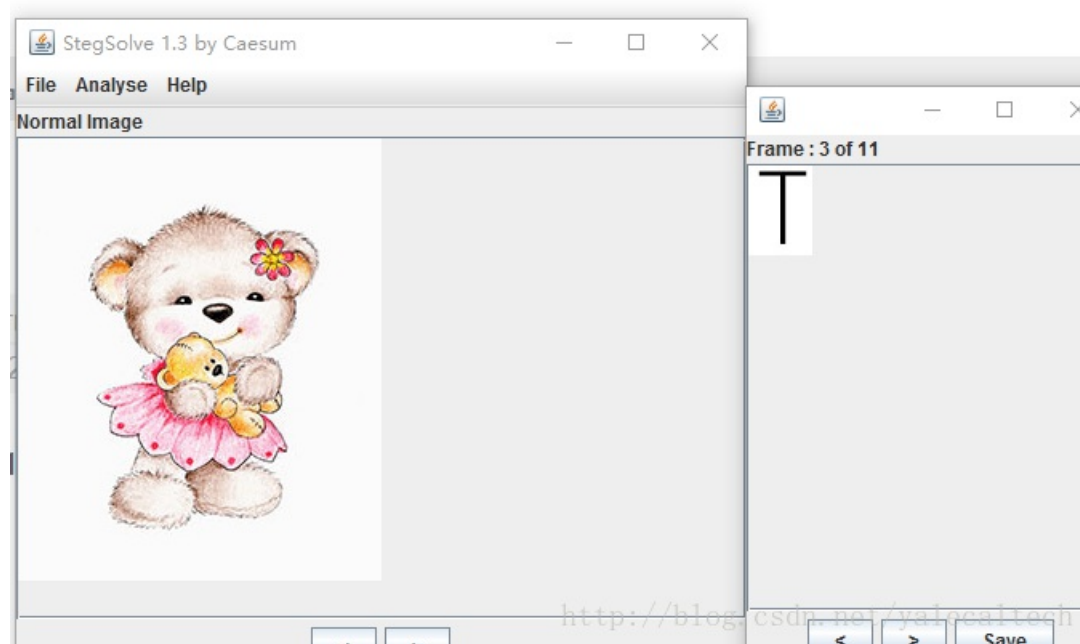
解压后得到png.zip

png是空白的, ss看看, 发现key



用其来解压zip, 得到gif,不过gif显示不出, 目测是少了文件头, 用winhex补16进制的文件头或者notepad++直接加GIF8也行, 保存后就可以打开了

发现是动图, 于是用ss的frame browser将图像一帧帧浏览, 得到flag

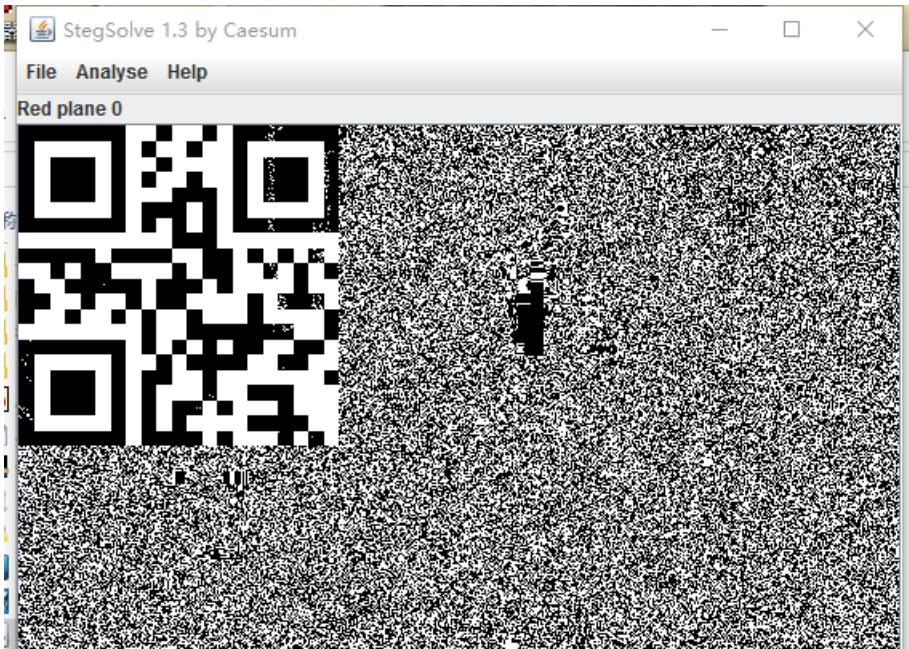
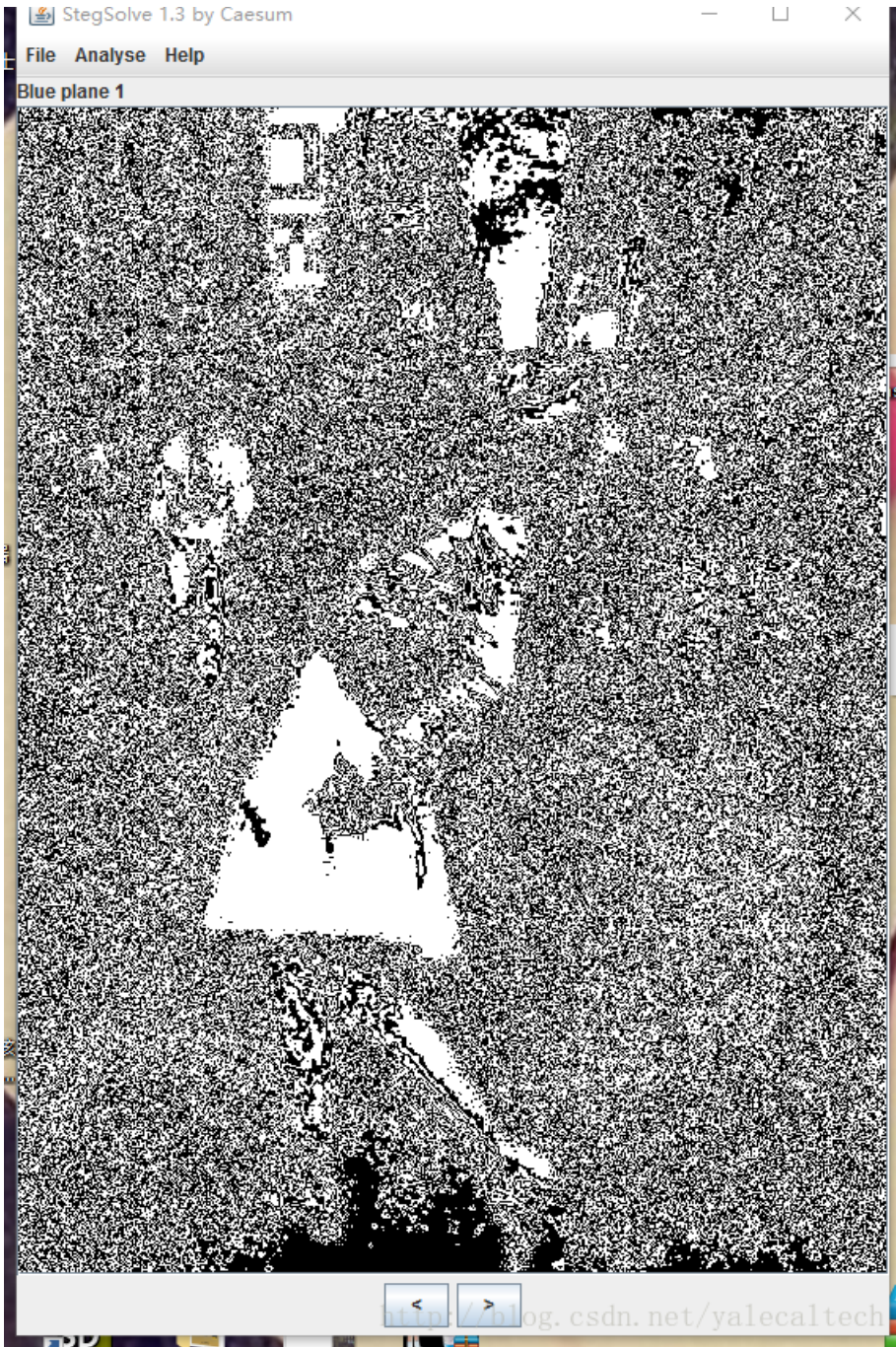


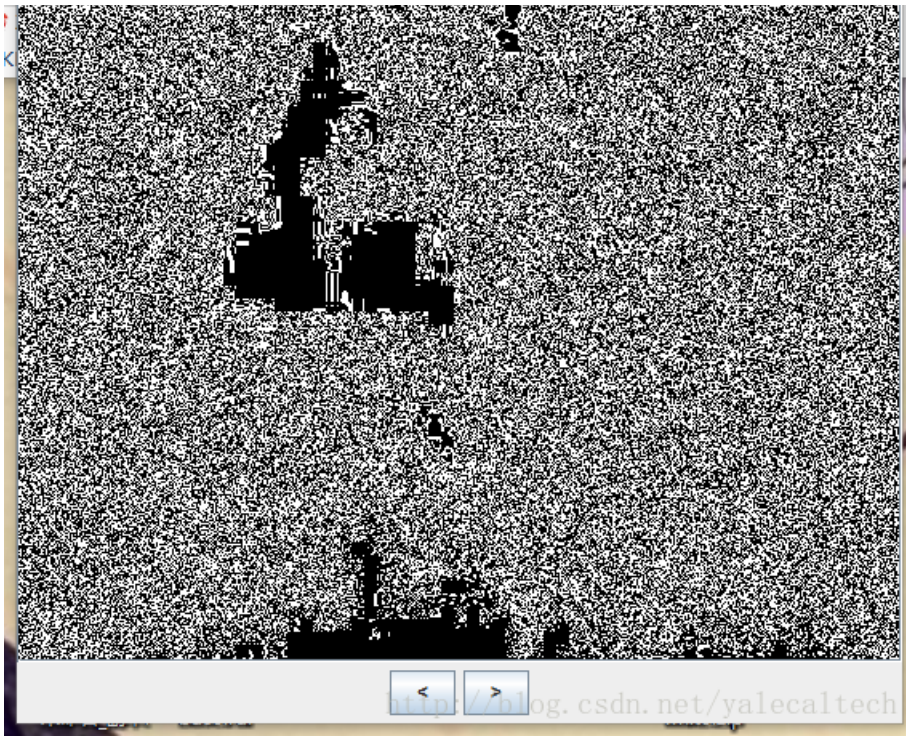
2.水果(<http://www.shiyanbar.com/ctf/1903>)

SS得到二维码, 扫描得到一串数字, 数字2位2位看发现大部分都重复了, 猜测可能是摩斯
于是先将数字转成ASCII再摩斯解密即可

3.最低位的亲吻 (<http://www.shiyanbar.com/ctf/1897>)

这题正常的套路应该是取出每个像素的最低位 (0或1按照0黑1白不行的话再反色) 来得到二维码
不过我们不走寻常路, 将bmp在画图中另存为png格式就可以了
因为我们png时偶然发现左上角有二维码的感觉, 才这么做的





4.无处不在的广告(<http://www.shiyanbar.com/ctf/1894>)

ss得到二维码，扫描得到结果

5.想看正面？那就要看仔细了！（<http://www.shiyanbar.com/ctf/1893>）

右键属性

| 属性 | 值 |
|-----------|-----------------|
| 说明 | |
| 标题 | 想看正面？那就要看仔细了！ |
| 主题 | 好吧，真的被你发现了！ |
| 分级 | ★★★★★ |
| 标记 | key is YmVhdXR5 |
| 备注 | key is YmVhdXR5 |
| 来源 | |
| 作者 | |
| 拍摄日期 | |
| 程序名称 | |
| 获取日期 | |
| 版权 | |
| 图像 | |
| 图像 ID | |
| 分辨率 | 510 x 453 |

base64解码即可

6.多啦a梦(<http://www.shiyanbar.com/ctf/1890>)

binwalk发现有两张图

```
kali:~# binwalk ameng.jpg
AL      HEXADECIMAL      DESCRIPTION
-----
0x0     Home             JPEG image data, JFIF standard 1.01
0x15A59 Desktop        JPEG image data, JFIF standard 1.01

kali:~# foremost -v -i ameng.jpg -o as
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
http://blog.csdn.net/yalecaltech
```

foremost提取出来

```
root@kali:~# foremost -v -i ameng.jpg -o as
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File

Foremost started at Sun Apr 2 12:53:06 2017
Invocation: foremost -v -i ameng.jpg -o as
Output directory: /root/as
Configuration file: /etc/foremost.conf
Processing: ameng.jpg
-----
File: ameng.jpg
Start: Sun Apr 2 12:53:06 2017
Length: 94 KB (97123 bytes)
                                KEY:SimCTF {ctfstega}

Num      Name (bs=512)      Size      File Offset      Comment
-----
0:       00000000.jpg      86 KB      0
1:       00000173.jpg       8 KB      88665
*|

Finish: Sun Apr 2 12:53:06 2017
http://blog.csdn.net/yalecaltech
```

打开图片得到flag

```
< KEY:SimCTF {ctfstega}
http://blog.csdn.net/yalecaltech
```

7.打不开的文件(<http://www.shiyanbar.com/ctf/1878>)

打不开基本上就是文件头的问题，先将它下载来，然后加上文件头GIF8

在用ss打开即可



得到是base64加密的，解码即可