攻防世界-Ditf

原创

xixihahawuwu 于 2020-09-10 09:43:56 发布 1808 收藏 1

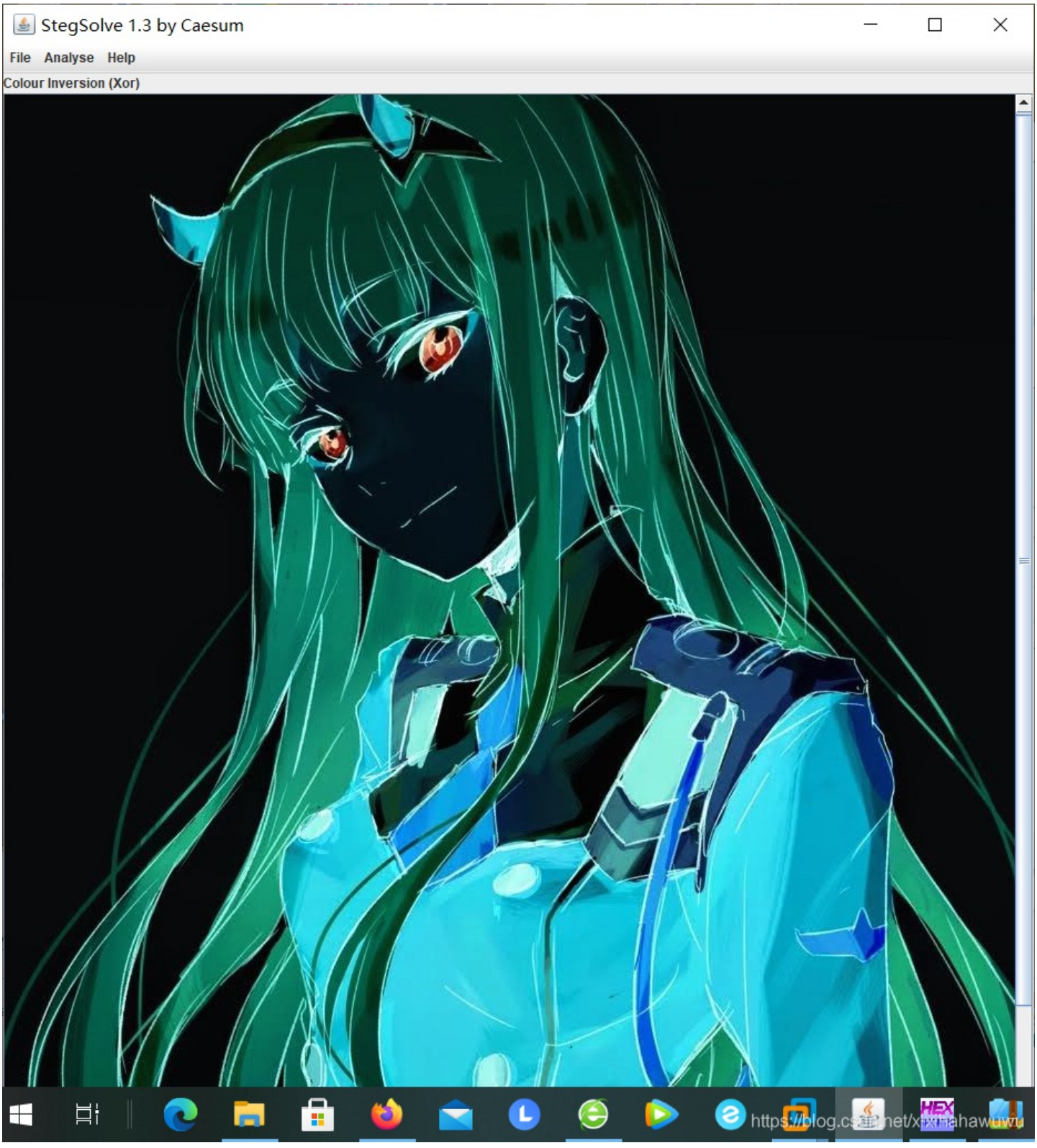
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/xixihahawuwu/article/details/108507588

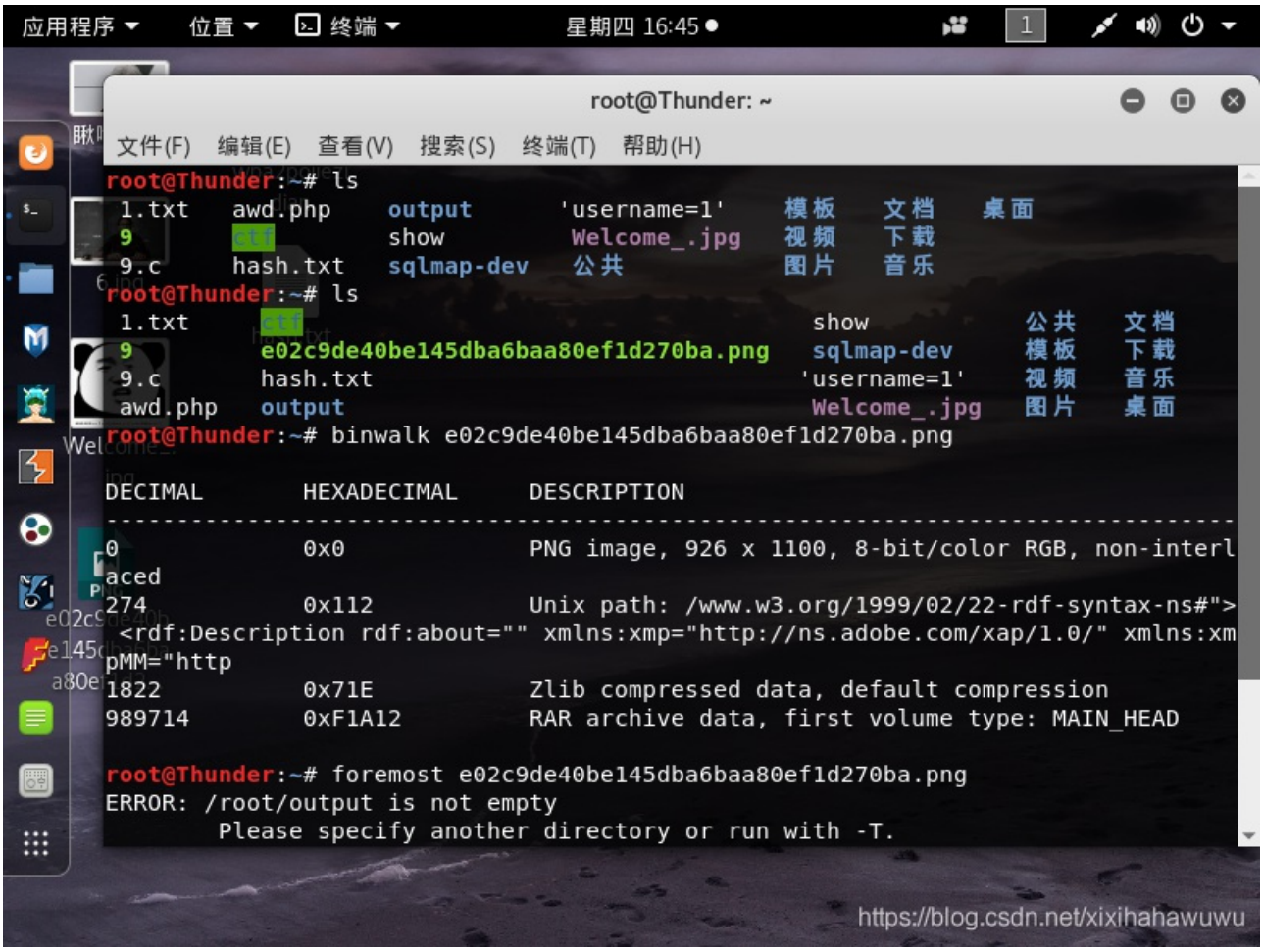
版权

题目下载下来是一个png文件

放入stegsolve中看，没有看出什么东西



把文件拖到kali中



Binwalk看下文件中是否包含其他文件

我们发现有一个压缩包

Foremost进行分离

得到压缩包后会发现需要密码

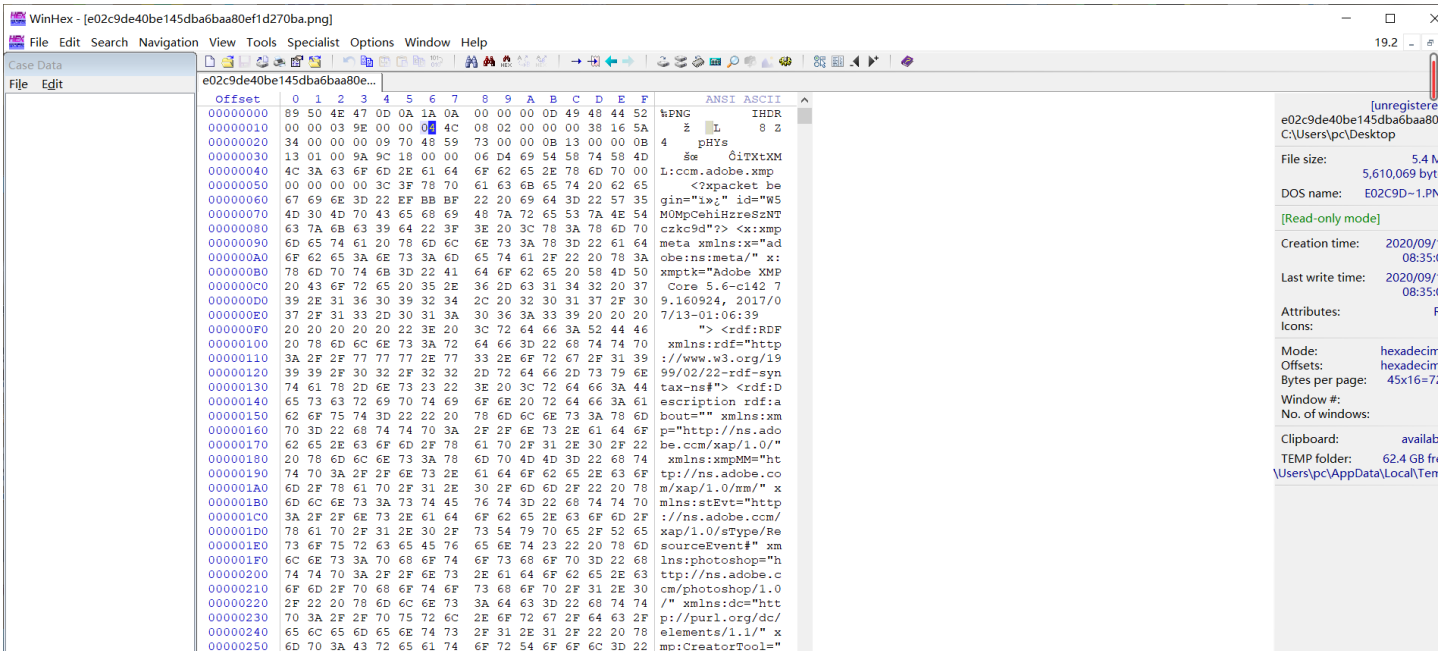
现在只能在png文件中找线索

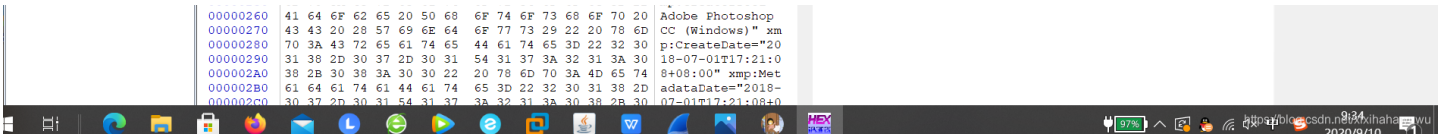
Stegsolve中没有看出什么

就到winhex中查看

还是没有找到什么明显的线索

于是想着会不会是修改文件的宽和高



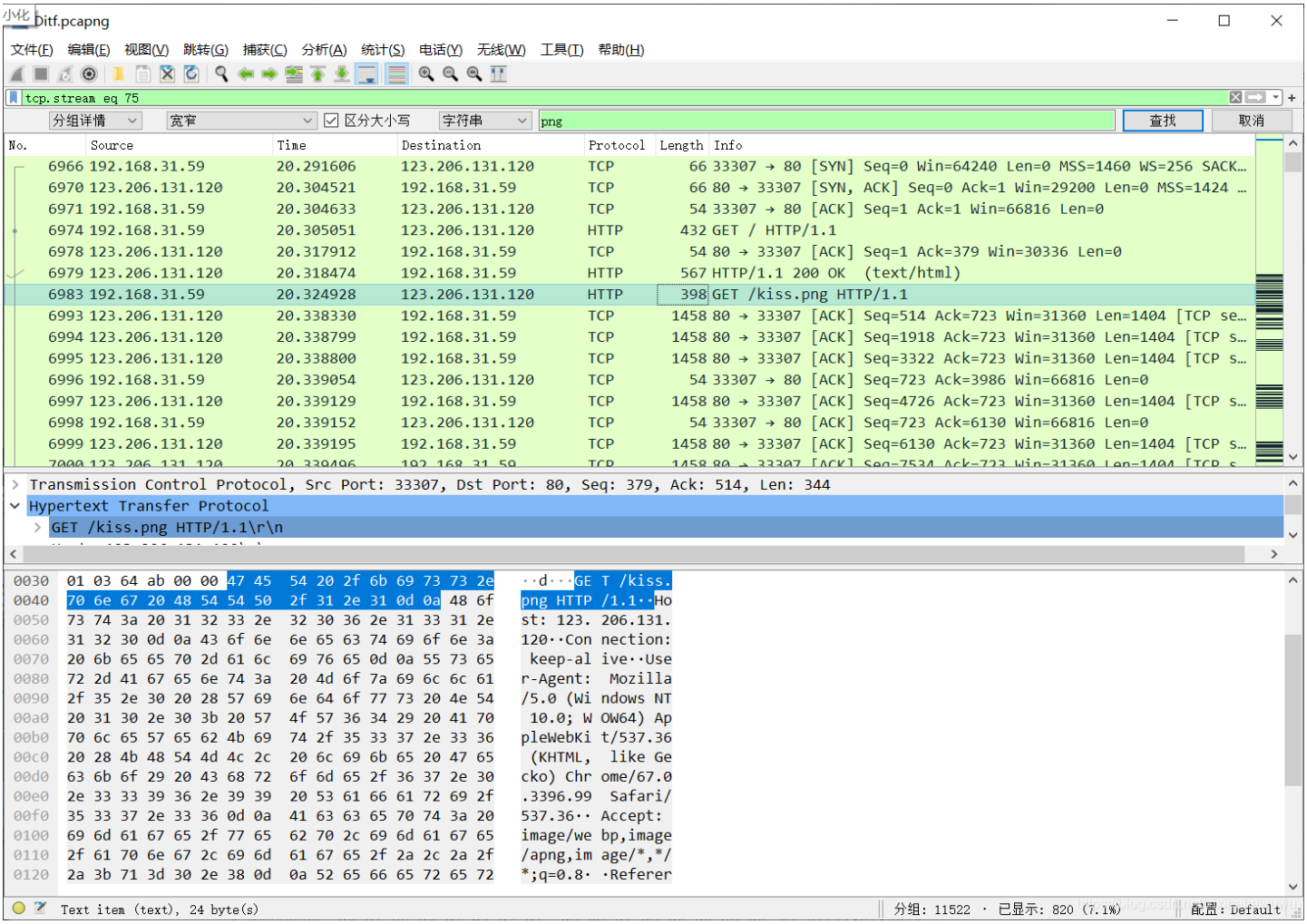


这里玩的软件不知道出了什么问题

没办法去修改，在我标记的地方修改为05后就可以看到图片下面出现了密码

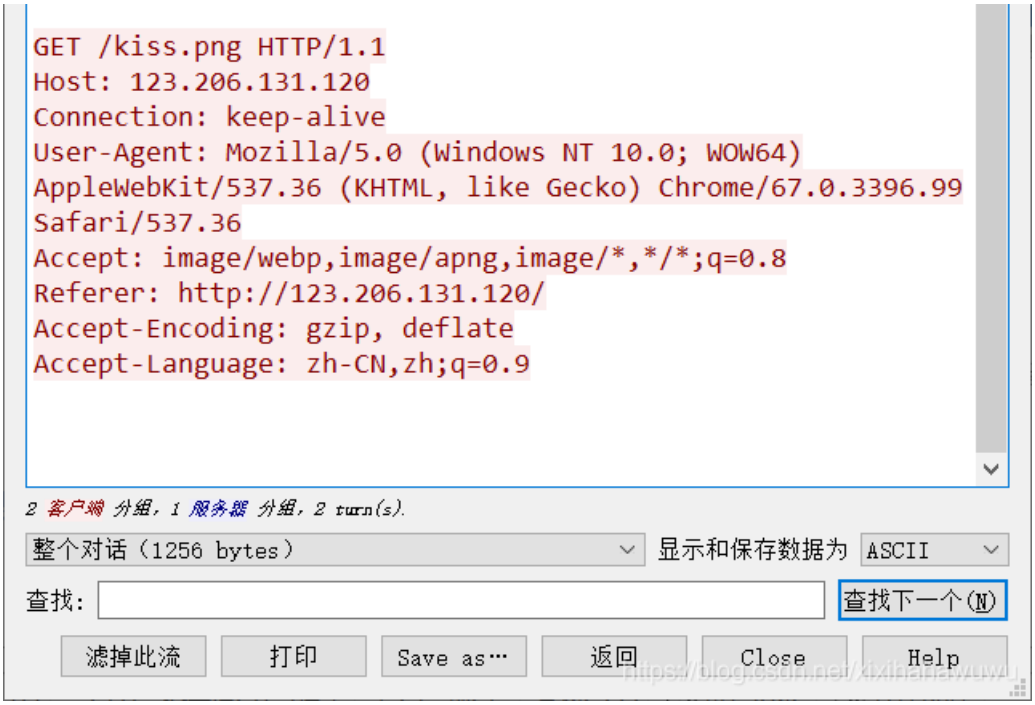
输入密码后得到了一个流量包

用wireshark打开



搜索关键字png后我们找到了一个png文件

在这里需要我们去追踪他的http流



我们会看到一个非常显目的base64加密
直接在线解密就好

这样就得到了我们的flag
flag{Oz_4nd_Hir0_lov3_For3ver}