xctf攻防世界 MISC高手进阶区 Ditf

原创

l8947943 于 2022-01-14 17:43:17 发布 3613 收藏

分类专栏： 攻防世界misc之路 文章标签： misc

本文链接：https://blog.csdn.net/l8947943/article/details/122498767

攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

1. 进入环境，下载附件

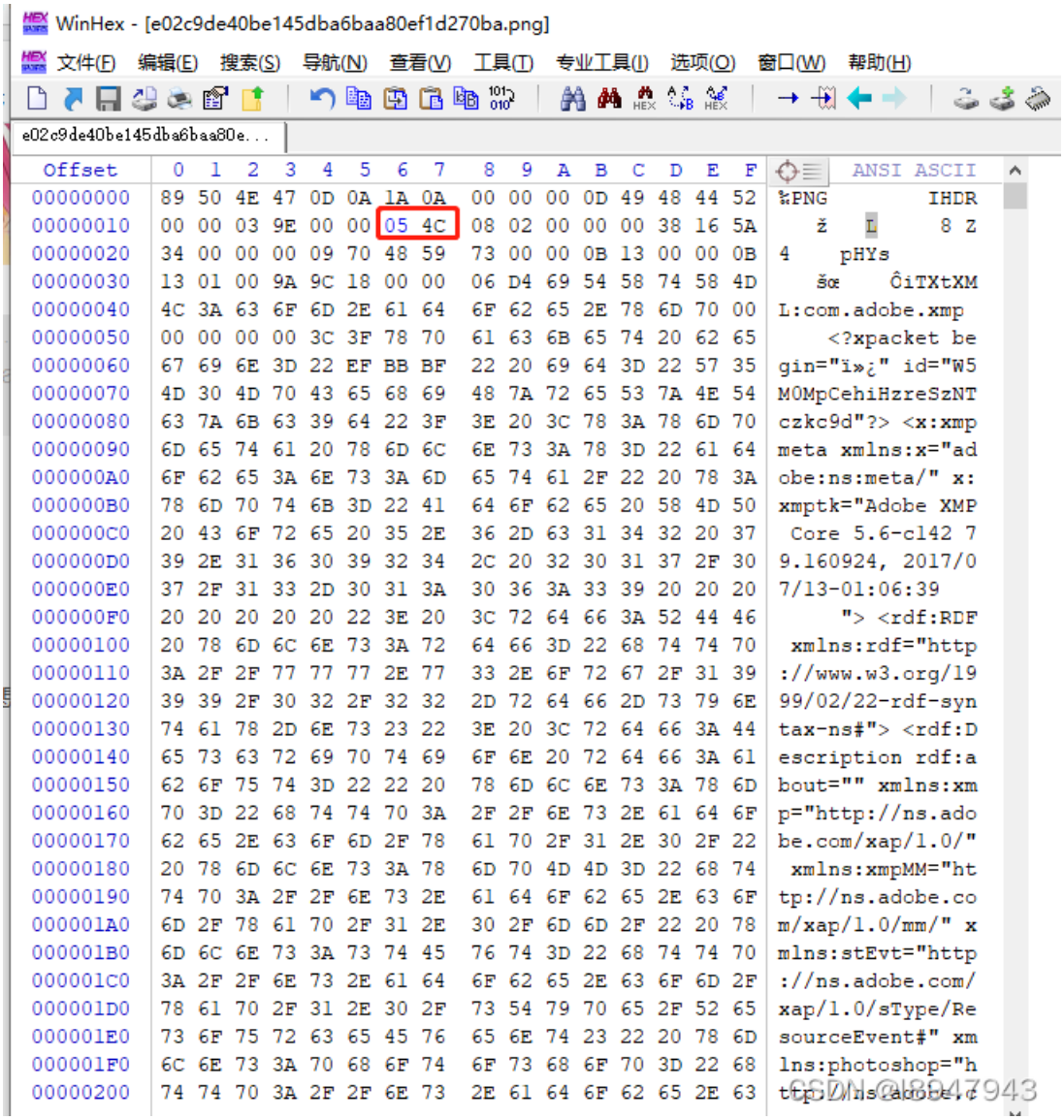
是一张美图：

没有其他提示信息，接着走。

2. 问题分析

1. **StegSolve探索**

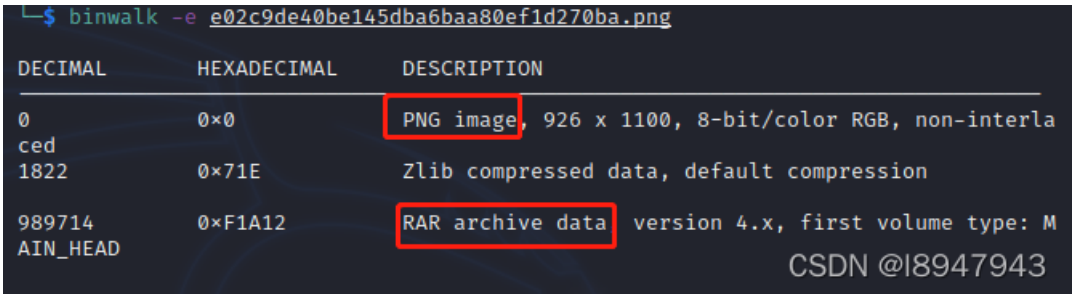
使用StegSolve打开图片，发现图片巨长。联想想到之前做的一个题，使用winhex修改图片高度



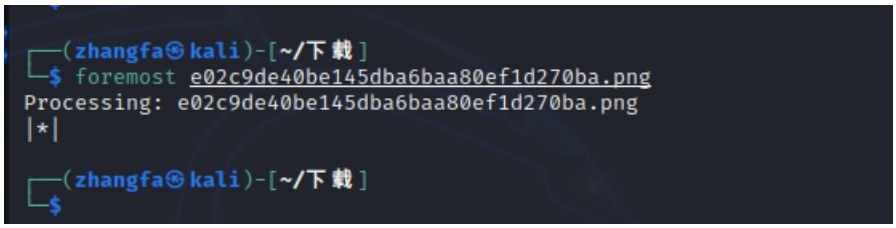
发现了隐藏的信息：

图片文件分离

我们将图片塞入kali中，使用binwalk查看一下，是否有隐含文件，如图：



有个rar文件，我们使用foremost分离一下，如图：

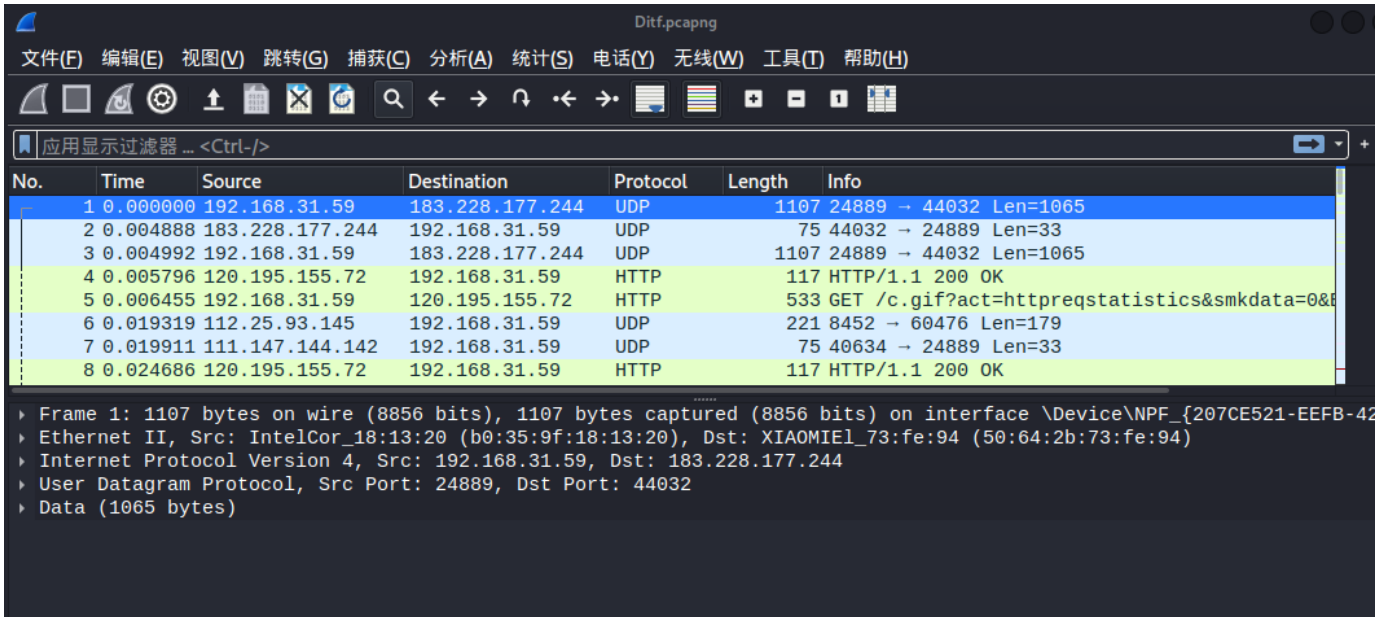


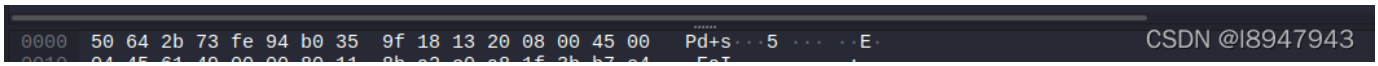
解密压缩包

解压过程发现需要密码，联想到刚才图片的字符StRe1izia，尝试一下：

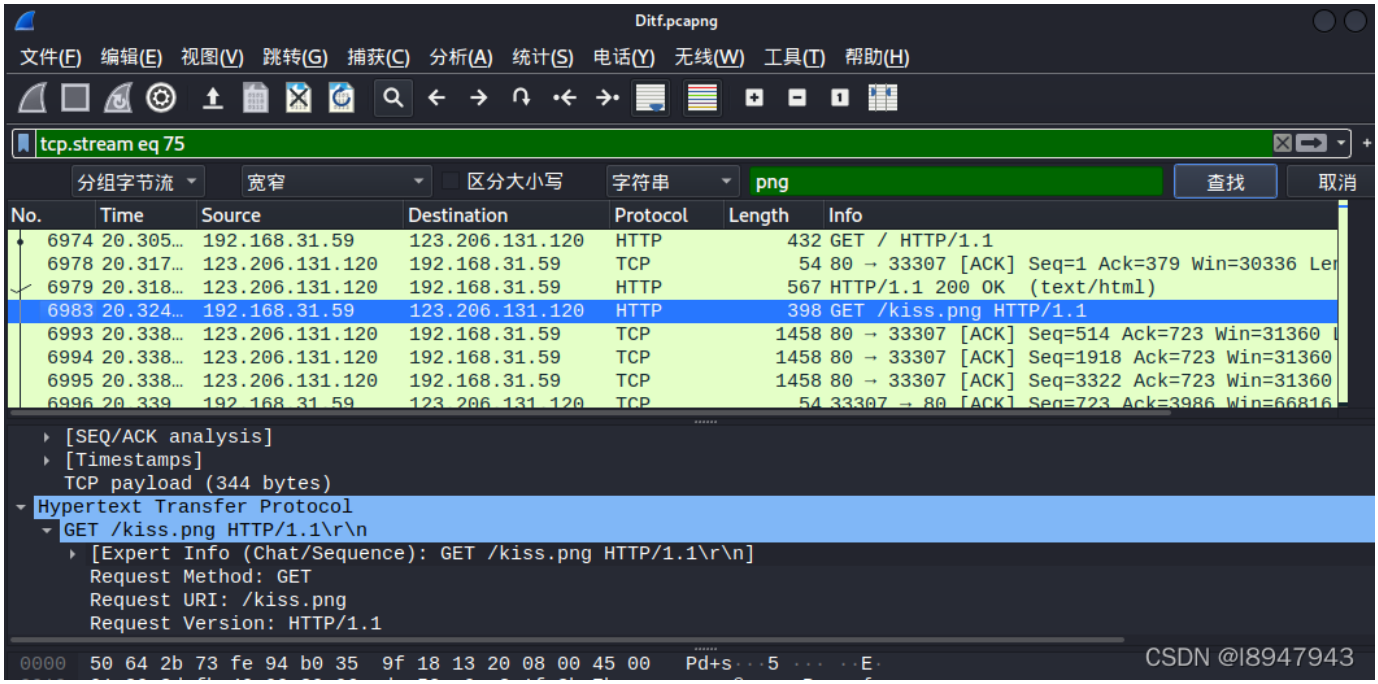
好家伙，还真解压成功了，是个pcag流量包文件，果断塞入wireshark，看看猫腻

分析数据流

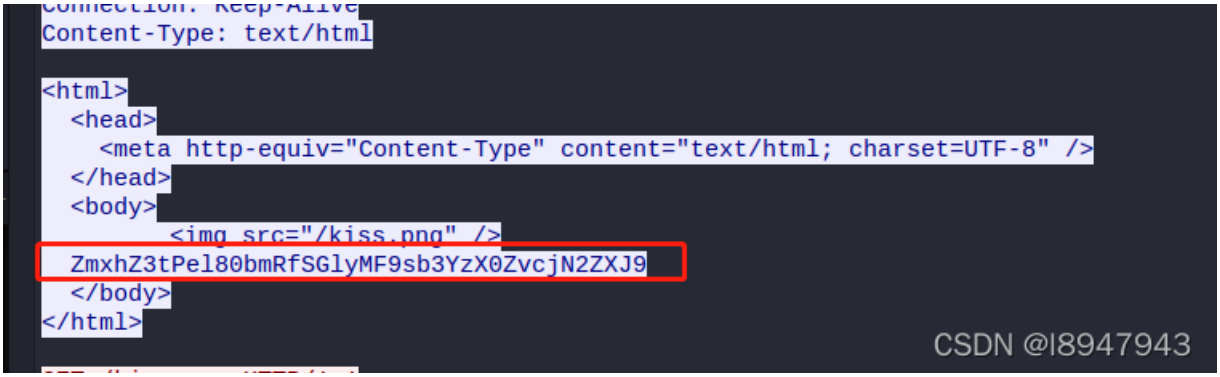




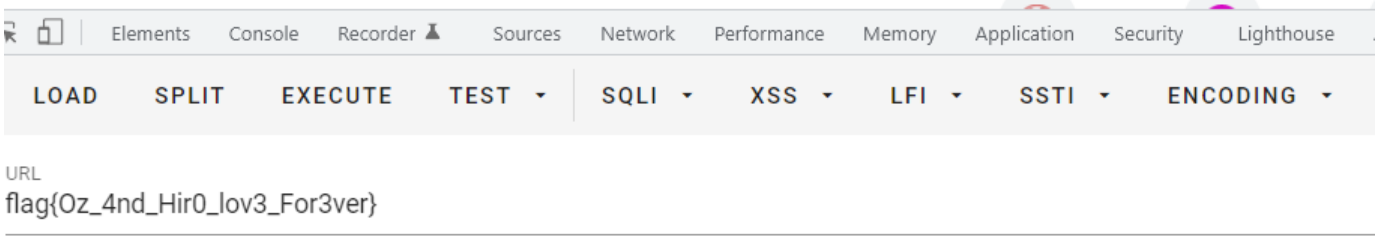
使用分组字节流搜索关键词flag和ctf，都没有对应内容！无思路了，查看wp，发现是要找png相关的关键词。。。如图：



追踪其http流，查看具体内容：



发现一串奇怪的东东（其实我也不知道为啥大佬们就知道这个是结果，o(╥﹏╥)o），使用base64解码，得到最终结果：



答案为：`flag{Oz_4nd_Hir0_lov3_For3ver}`