# xctf攻防世界 MISC高手进阶区 flag_universe

原创

l8947943 于 2022-01-17 20:26:10 发布 5579 收藏 1

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/122547543



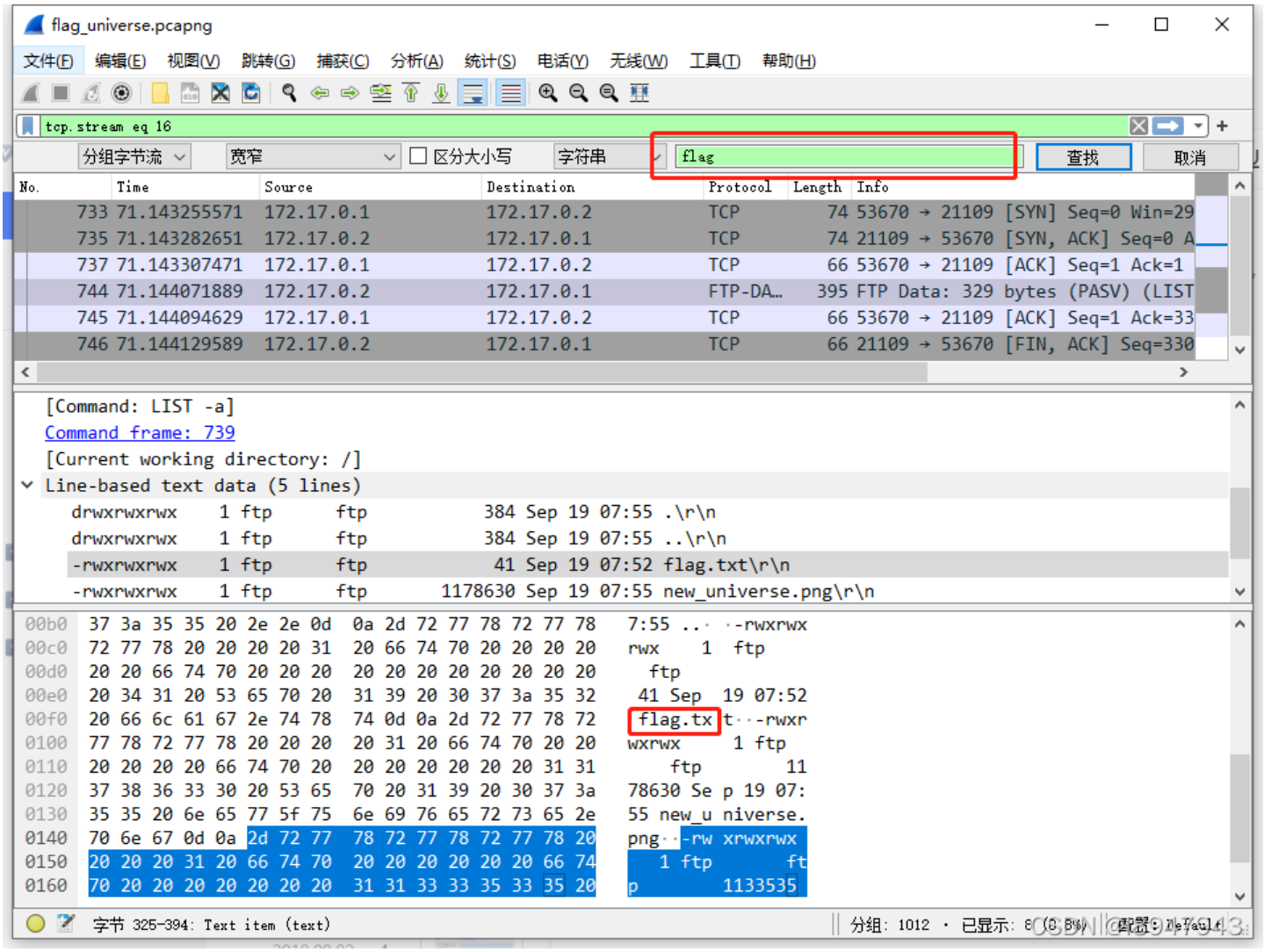
攻防世界misc之路 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

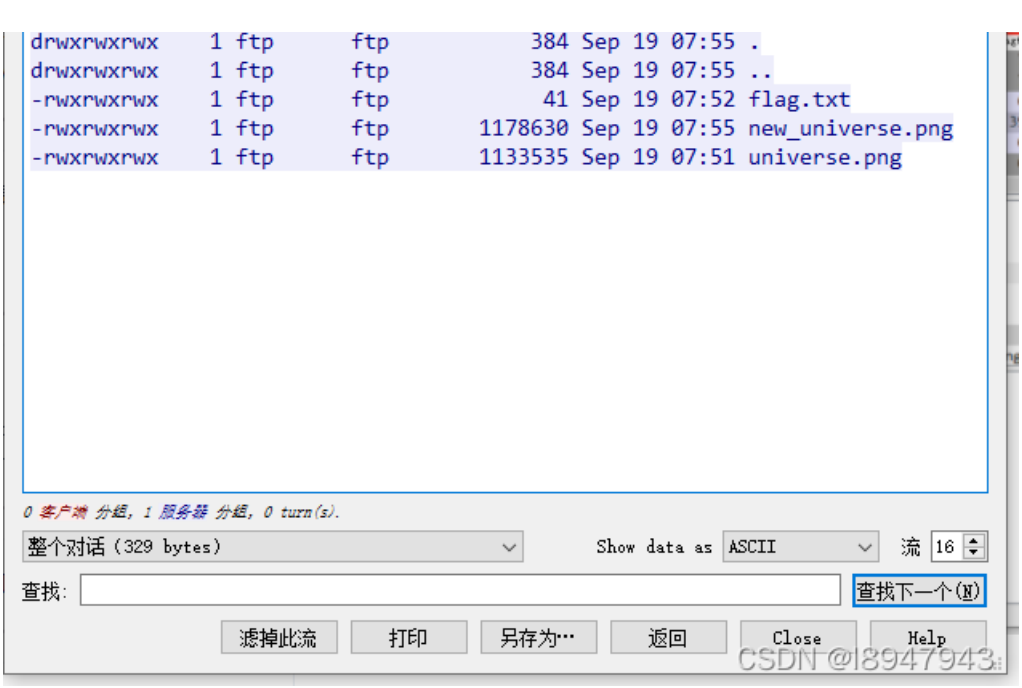
## 1. 进入环境，下载附件

下载后，给的是pcapng文件，果断使用wireshark打开，在其中搜索关键词flag，发现如下：




## 2. 问题分析

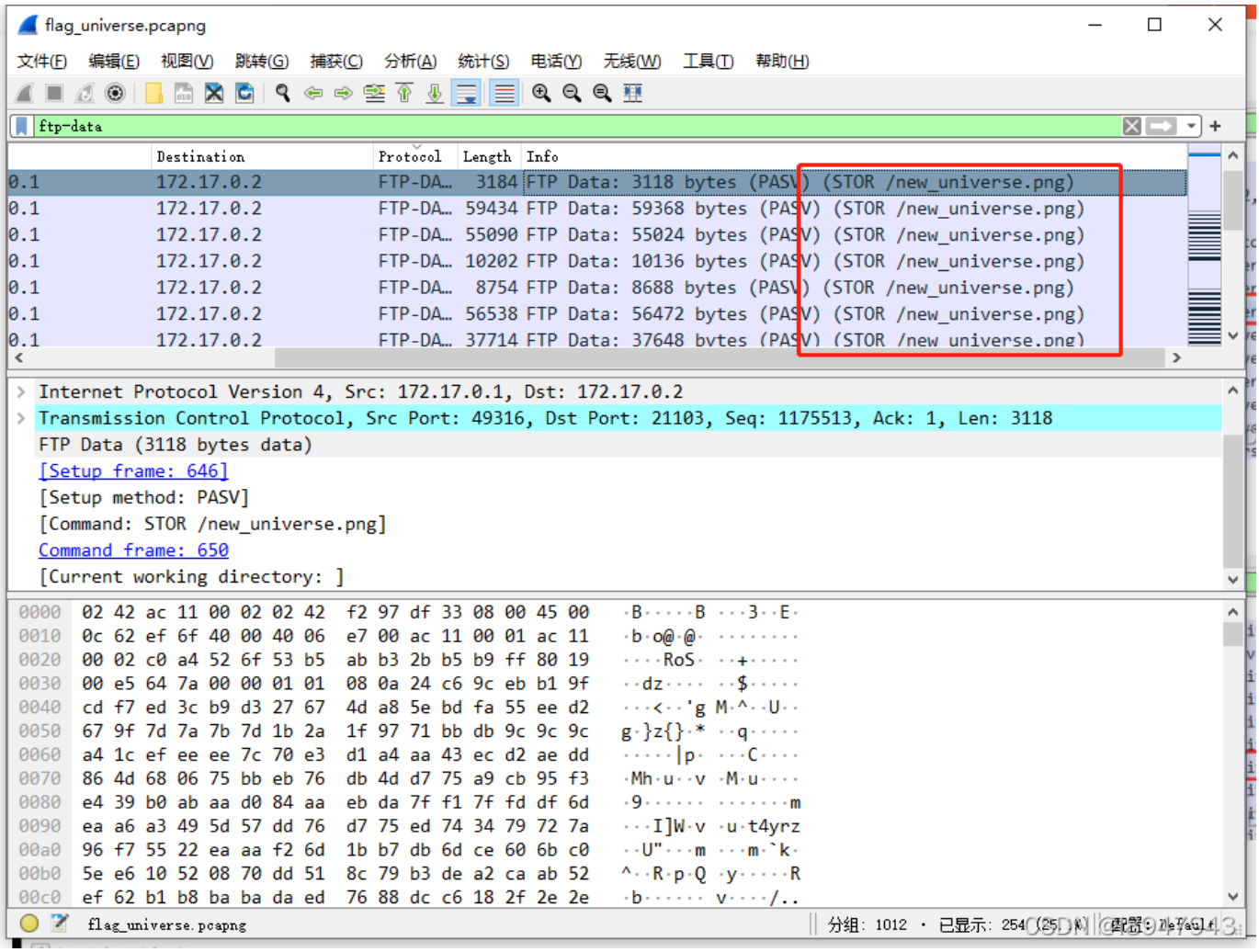
追踪流




可以看到，采用的ftp协议，对文件flag.txt、new_uniberse.png和universe.png文件进行了上传，因此，解题关键是把上传的图片给还原出来。

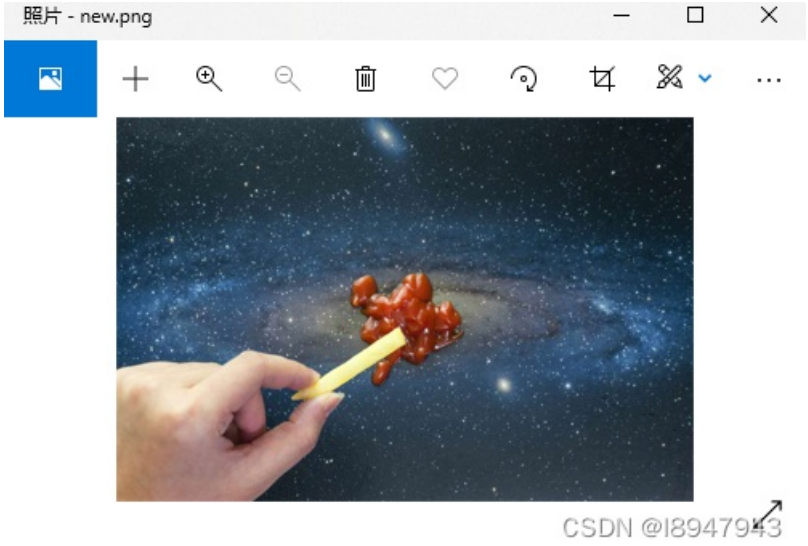
**找到new_uniberse.png**

如图：




把找到的上传图片追踪流导出来，在这里推荐使用工具用NetworkMiner打开流量包，他妈的电脑安装后缺少什么dll文件，人麻了，手工导出吧。

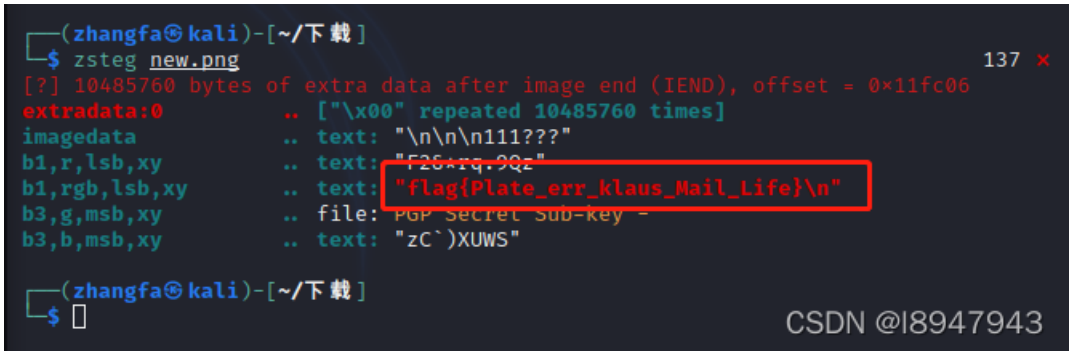
追踪流，复制原始数据，到winhex中建立10MB的文件并粘贴进去，最终以为png文件命名。如图：




### 使用zstag隐写发现

先安装工具，参考博客：https://www.cnblogs.com/lzkalislw/p/12831430.html

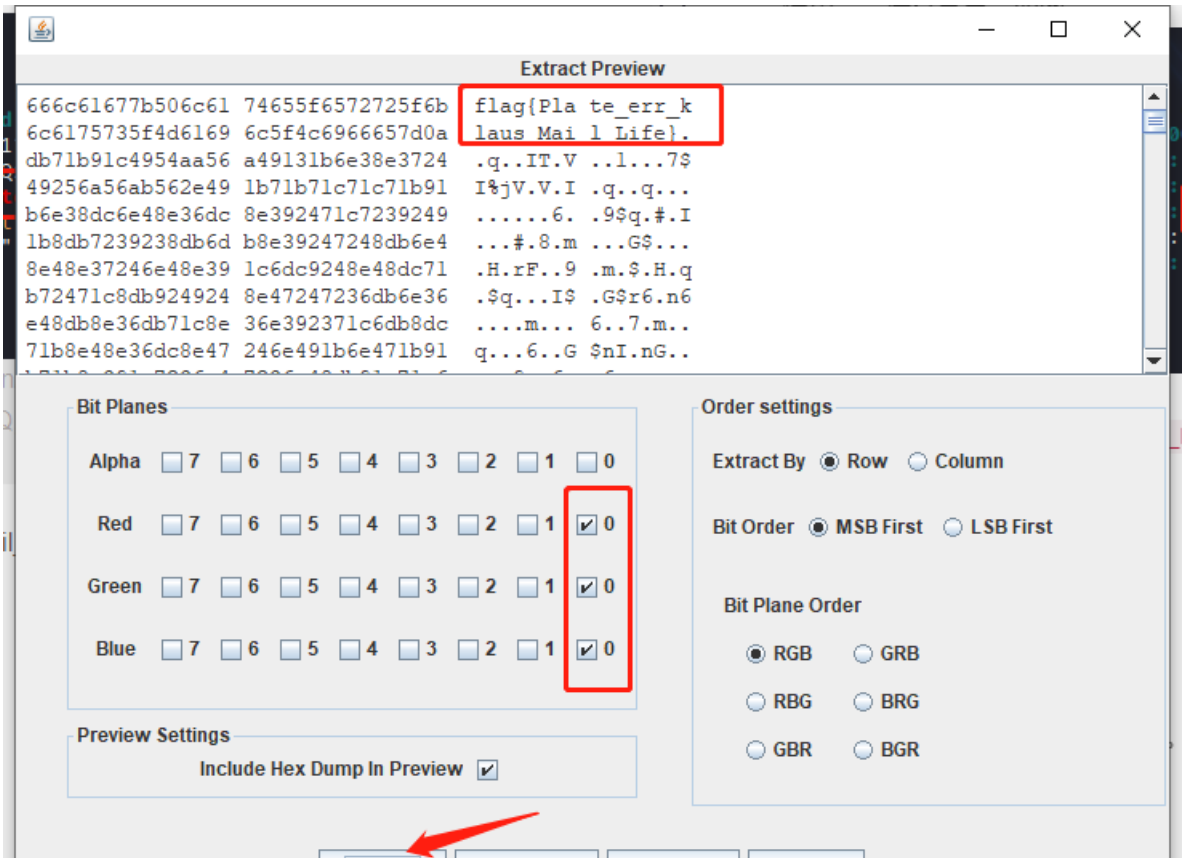
使用命令进行分离，如图：

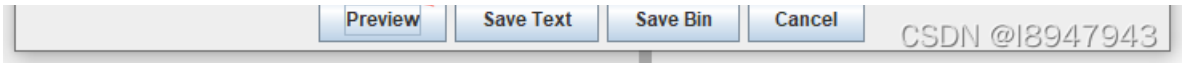



得到最终的答案：`flag{Plate_err_klaus_Mail_Life}`

### StegSolve发现隐写

如图，该工具也可以找到隐写：






## 3. 总结

- 隐写工具使用（第一次接触zstag。。。）
- 追踪流并得到传输文件

这个题学到东西了，欢迎交流~~~