攻防世界 flag_universe

原创

方亭子 已于 2022-03-02 09:33:45 修改 2344 收藏

分类专栏： # 攻防世界MISC题目 文章标签： 安全

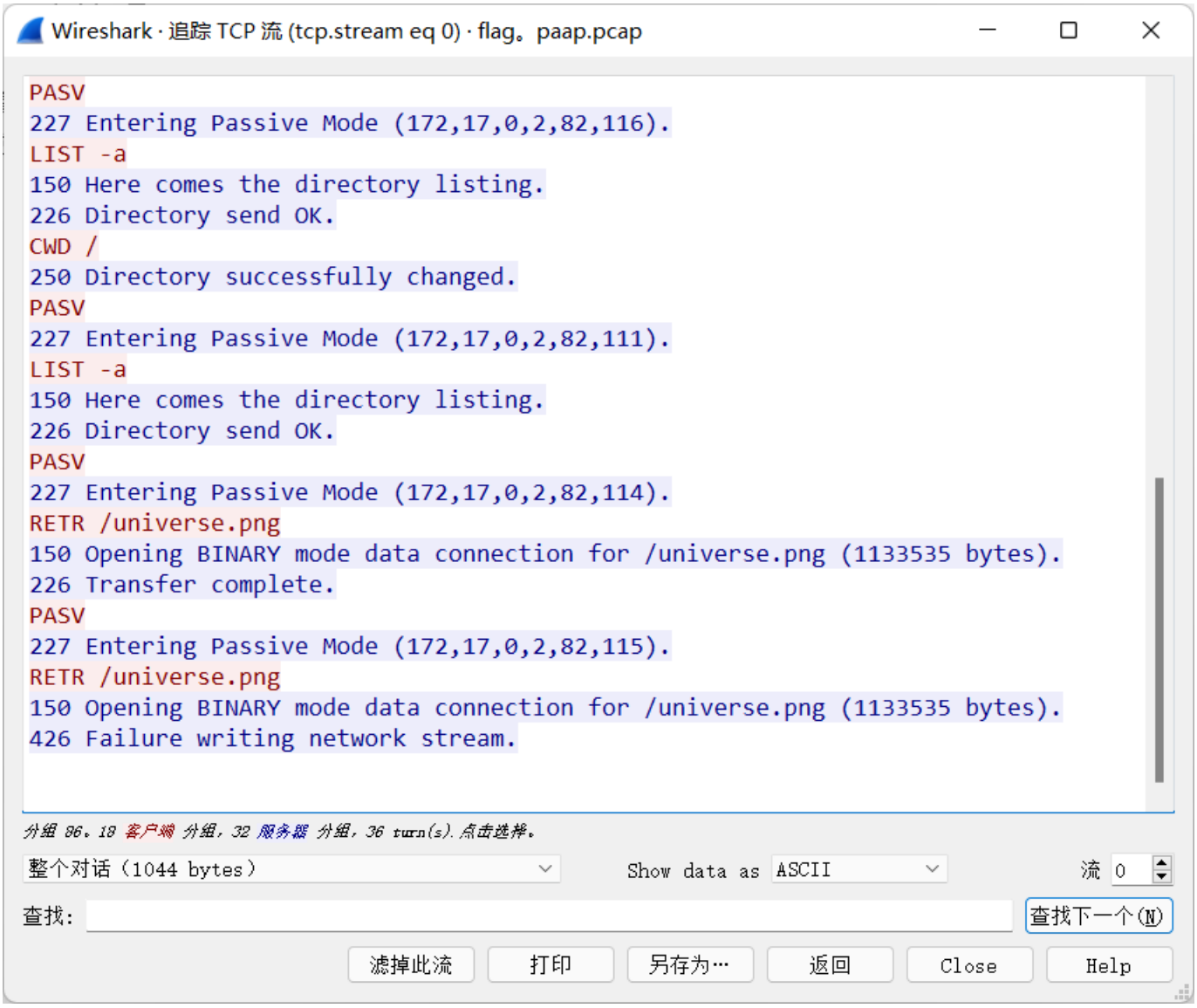
于 2022-02-24 20:52:46 首次发布

方莱莱出品

本文链接：https://blog.csdn.net/weixin_46342884/article/details/123120787

拿到题目，解压后是一个pacpng格式的流量包

使用wireshack打开后追踪tcp数据流。可以看到这是通过PASC上传的图片



继续追踪数据流
在流2里面可以看到上传的文件

```
drwxrwxrwx    1 ftp      ftp           264 Sep 19 07:52 .
drwxrwxrwx    1 ftp      ftp           264 Sep 19 07:52 ..
-rwxrwxrwx    1 ftp      ftp            41 Sep 19 07:52 flag.txt
-rwxrwxrwx    1 ftp      ftp       1133535 Sep 19 07:51 universe.png
```

在流7里面发现一串base64字符，解码后发现是假的flag

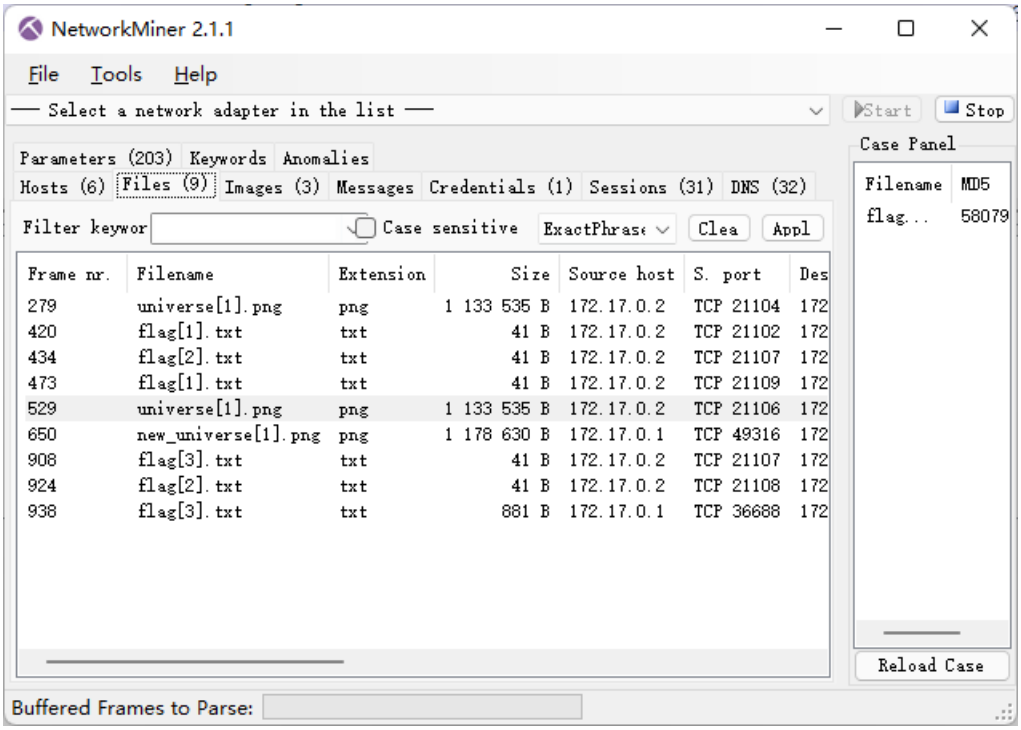

```
<<< 选择 >>>
--加密--
--解码--
--退出--
: 解码
base64解码: ZmxhZ3tUaGlzIGlzIGZha2UgZmxhZyBoYWhhaGF9
**********Decoding complete**********
: flag{This is fake flag hahaha}
****************************************
```

判断flag藏在这些上传的文件中

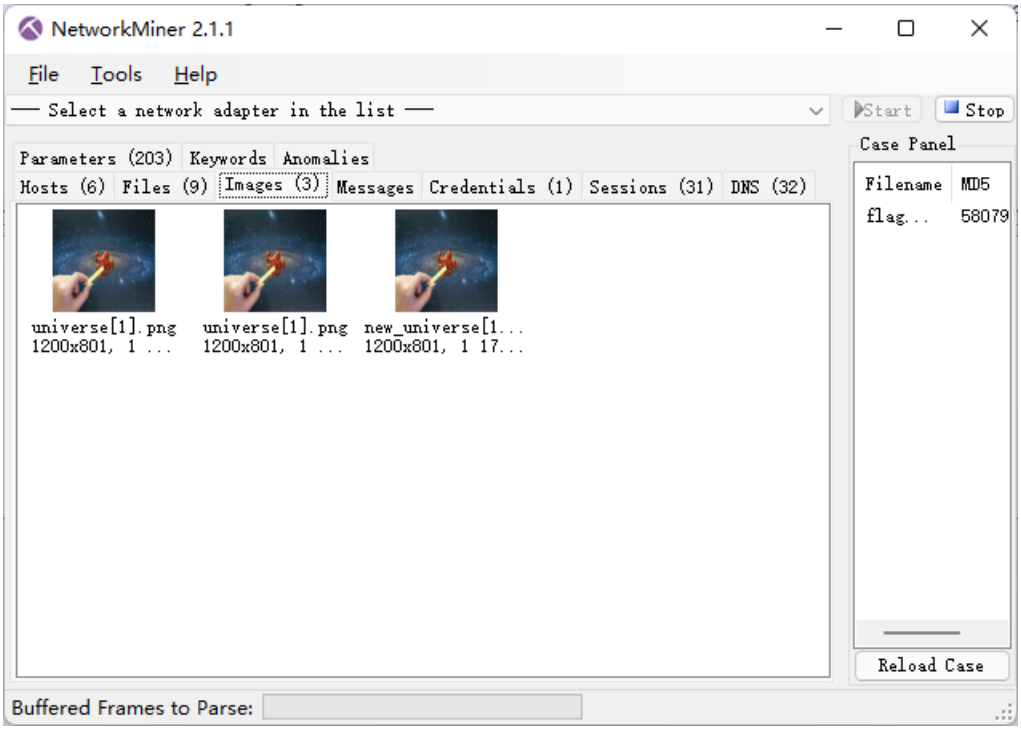
使用工具networkminer打开流量包，提取图片

注意，需要先用wireshack把流量包另存为格式为pacp的文件，因为pacpng文件需要正式版才可以打开

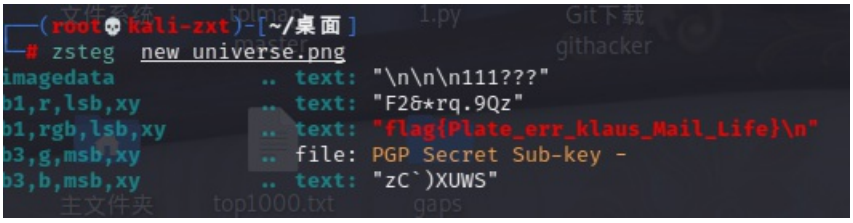
打开后，可以看到上传的文件



找到图片



这里的flag.txt打开后是我们原先解码的假的flag
右键打开图片位置，保存后使用setgsolve查看，没有发现什么线索
放到kali里面使用binwalk查看，也没有发现什么，使用zsteg检查是否有隐藏数据
发现flag



这里推荐一个软件networkminer网络数据分析工具，可以很好的检查流量包文件