Buuctf 被偷走的文件

原创

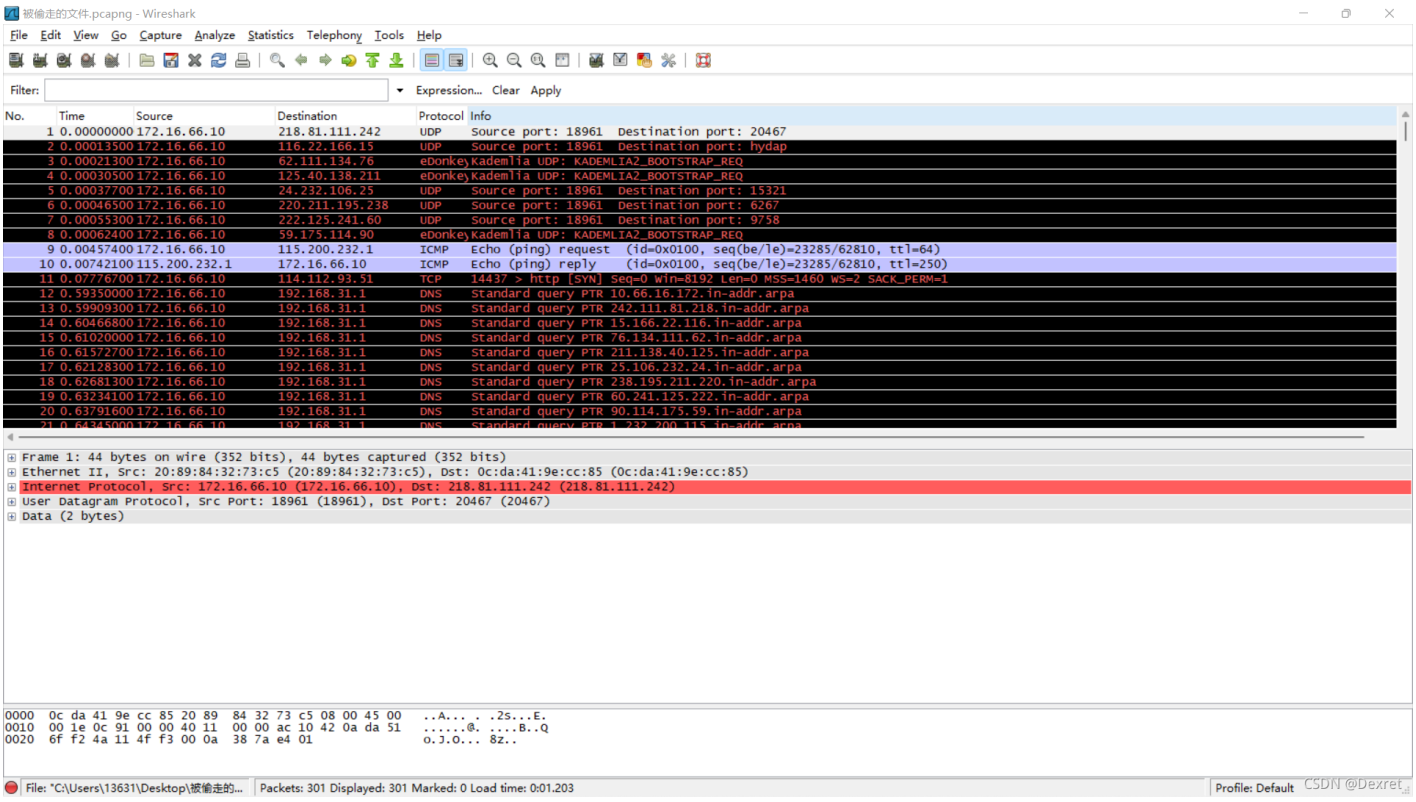
Dexret 于 2021-11-22 19:55:31 发布 1083 收藏
分类专栏： Buuctf Misc 文章标签： 安全 加密解密 wireshark

本文链接：https://blog.csdn.net/Dexret/article/details/121476617


Buuctf Misc 专栏收录该内容
47 篇文章 0 订阅
订阅专栏

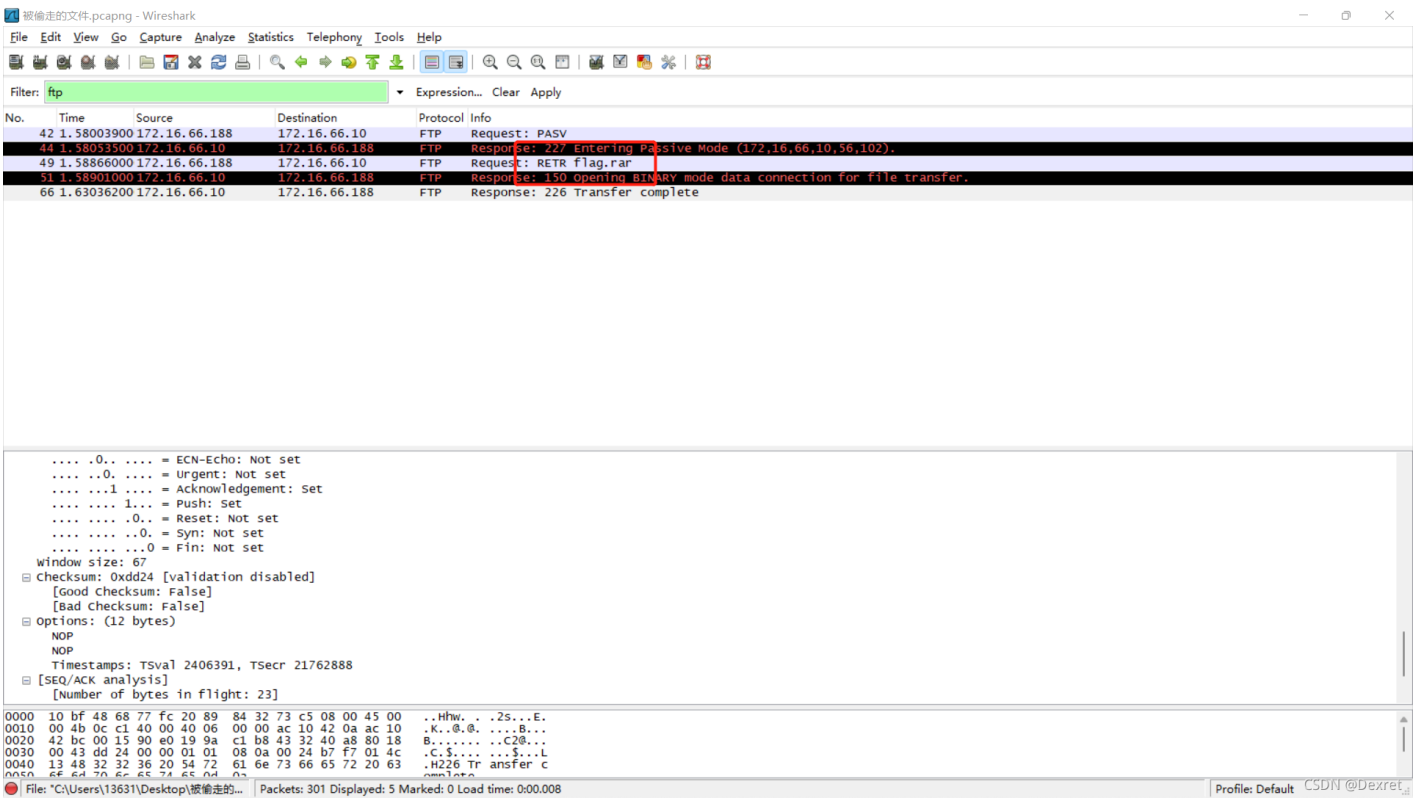
下载该文件，发现该文件为一个流量包文件

通过wireshark打开该文件



通过题意得知该题需要我们分析被盗走的文件

在该数据包中看到有ftp传输，过滤ftp数据包

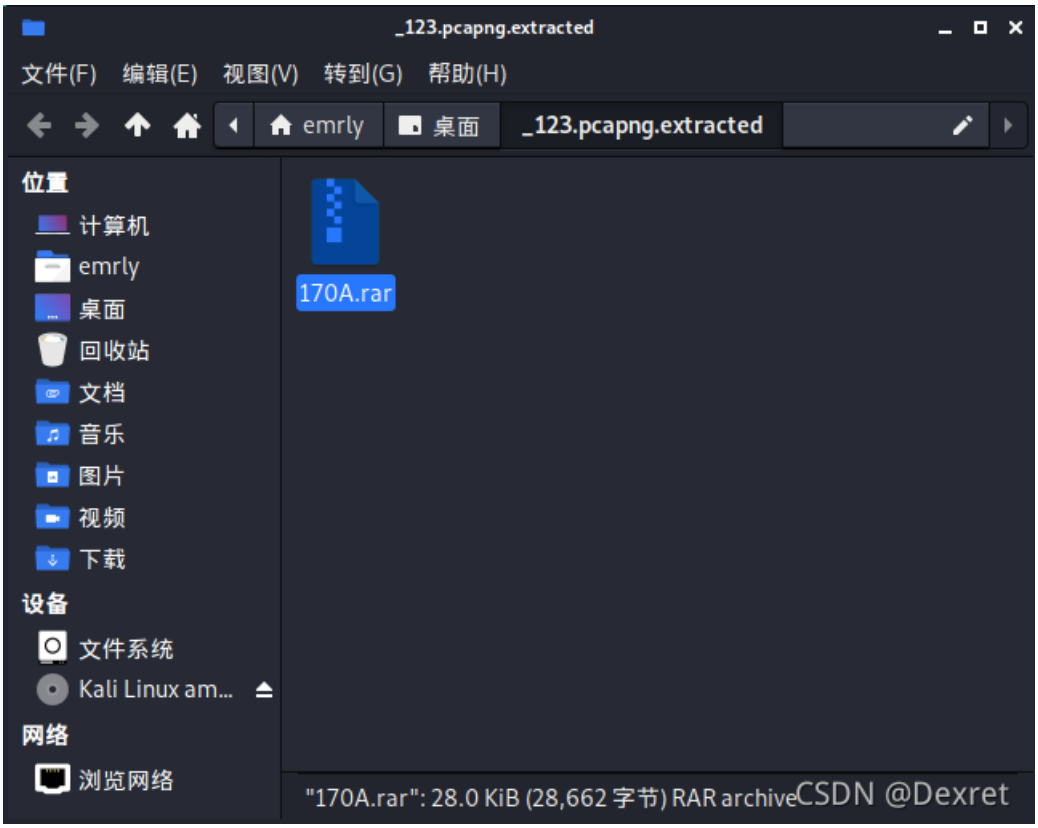


可以看到ftp传输有个flag.rar文件

通过kail中的binwalk对该文件进行分离(这里改了下名称，容易分离出来)

```
binwalk -e 该文件名称
```

分离得到一个压缩包文件

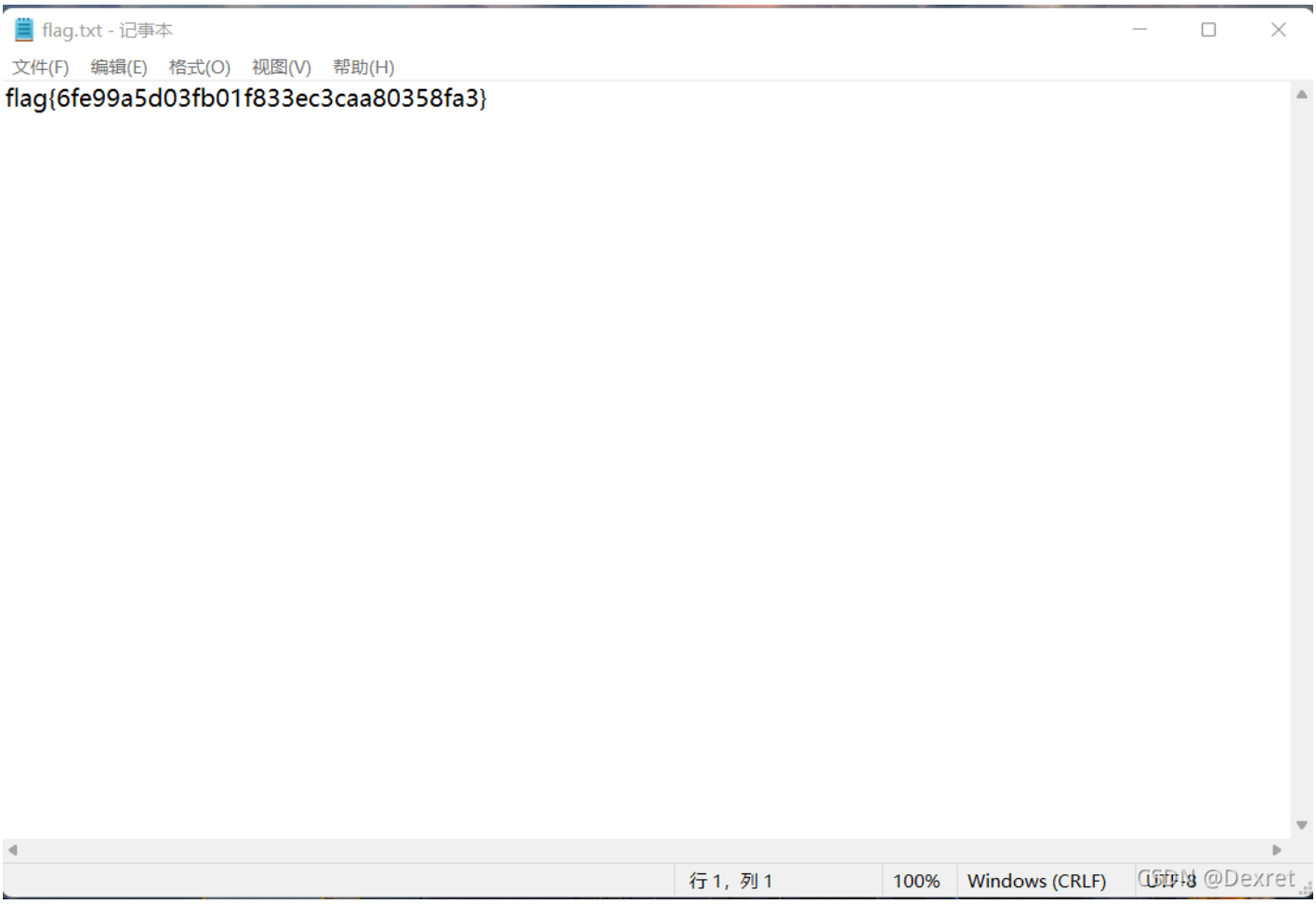


打开压缩包文件发现该压缩包文件有密码

利用ARCHPR对该文件进行密码爆破

最终得到该压缩包密码为：5790

通过该密码成功解压压缩包，发现里面有个flag.txt文件，将其打开



成功获取到该题的flag：

```
flag{6fe99a5d03fb01f833ec3caa80358fa3}
```