**数据包取证总结**

1. 先观察题目，如果题目有明确指示某端口，或某协议。然后根据提示的端口和协议构造过滤表达式，否则话一般都是考http协议的那种 （wireshark打开数据包后，使用了过滤表达式后先搜索一下关键字flag，如果简单的题话会有flag）

题目：BUUCTF-Misc-sqltestfl

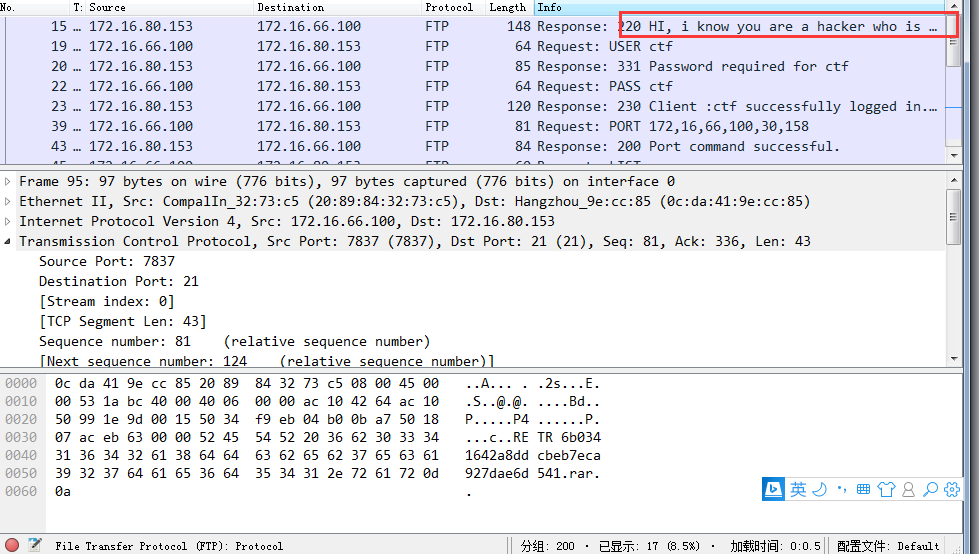
1. 如果题目有类似于BUUCTF-Misc-sqltest这种类型的，二话不说wireshark打开数据包后，直接导出全部为html，根据题目来获取flag

参考文档：第一届HappyCTF大赛WriteUp.pdf

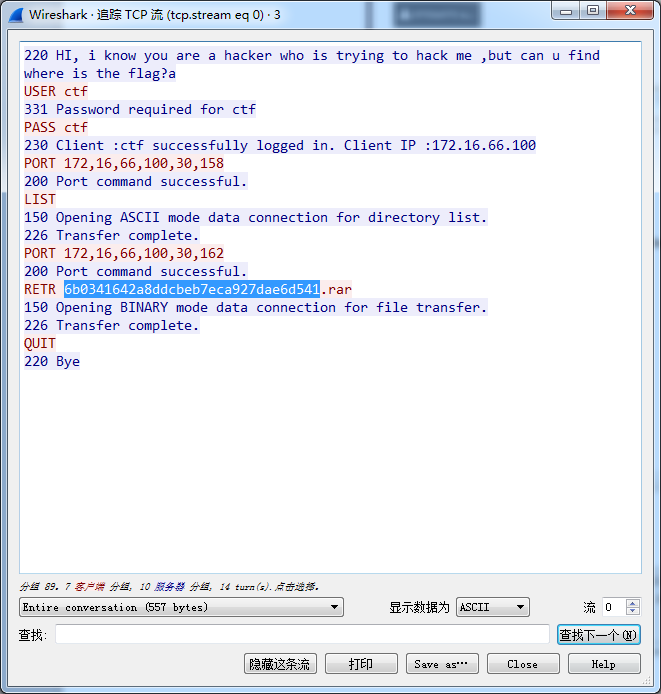
特殊的题目：BUUCTF-Misc-秘密文件。给你一个数据包，然后题目的要求是：



Wireshark打开后，我一开始以为是http流量。因为之前的题才是流量，后面我在某条数据见到一些字

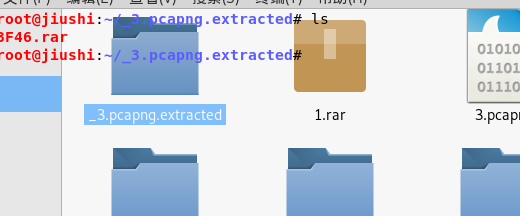


后面发现是FTP流量，查看tcp流。发现一些提示



这里说明了，Hacker是通过登陆FTP，然后下载了一个rar文件。后面我想了很久。也试过导出分组节流作为zip，后面发现根本不是。后面在某篇文章上面见到对数据包binwalk的，后面我也对这个数据包进行binwalk。然后还真的藏着一个压缩包

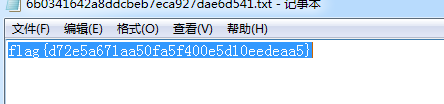
文章地址：<https://www.addon.pub/2018/04/10/CTF%E4%B8%AD%E7%9A%84%E6%9D%82%E9%A1%B9%E5%B0%8F%E7%BB%93/>



后面尝试对这个rar输入ftp登录的密码，发现不对。拉到windows进行爆破，ok得到密码



解压压缩包即可获得flag



一条可以从数据包里列出所有隐藏文件的命令： Tshark

Tshark -r out.pcap -T fields -e data > out.txt

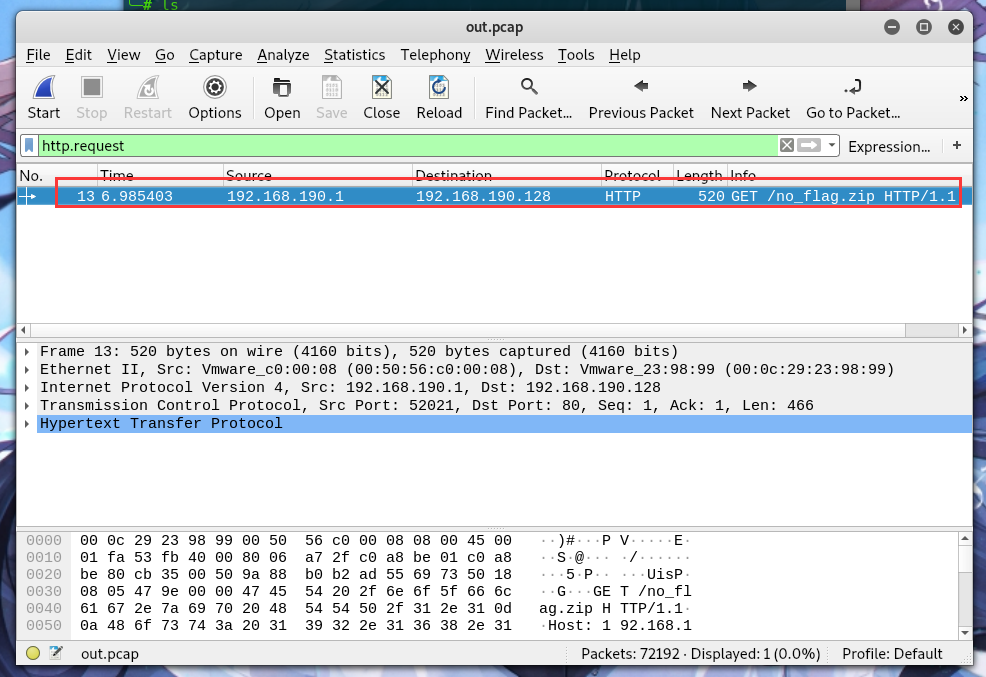
删除重复数据的命令:uniq

Uniq demo.txt

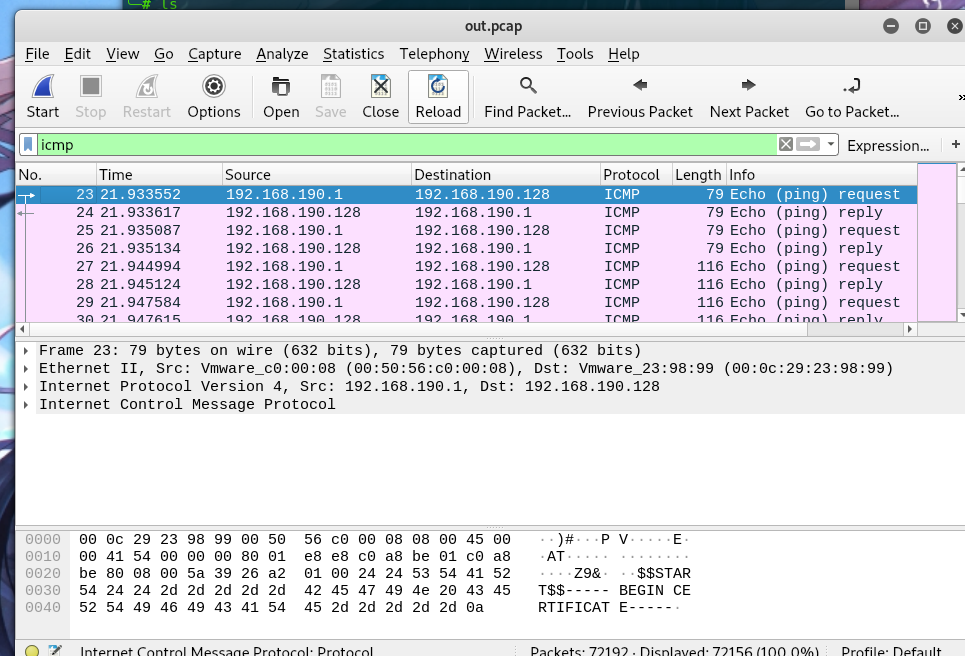
特殊的题：BUUCTF-Misc-蜘蛛侠

首先一开始我呢，我去搜http.request。发现只有一个not\_flag.zip

也就只有那一条数据



后面我在imcp看见结尾有base64

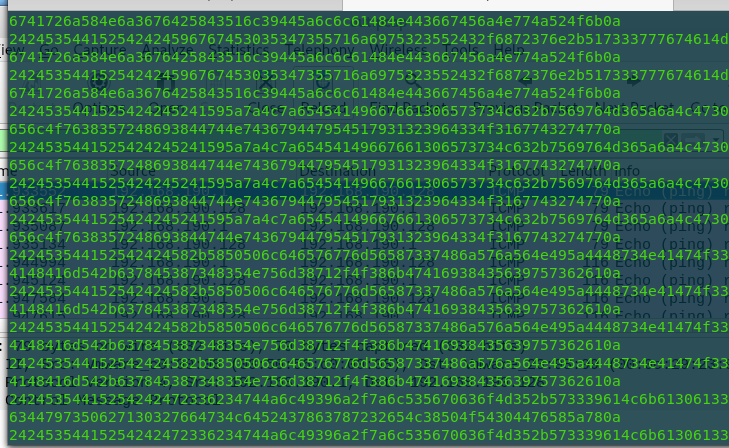


一开始以为不是，后面看了WP之后那个就是。。。，后面根据WP学到了一条命令

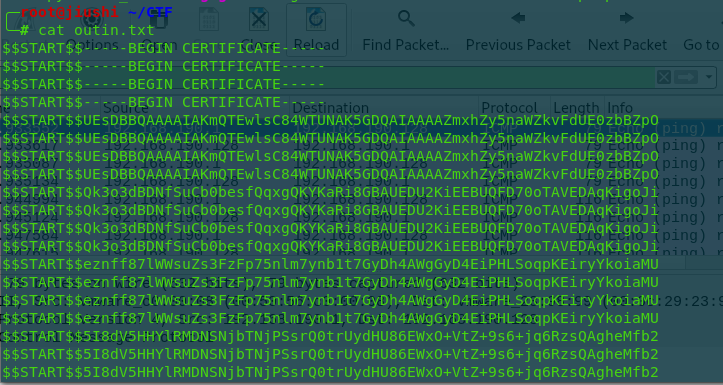
一条可以从数据包里列出所有隐藏文件的命令： Tshark

Tshark -r out.pcap -T fields -e data > out.txt

得到out.txt

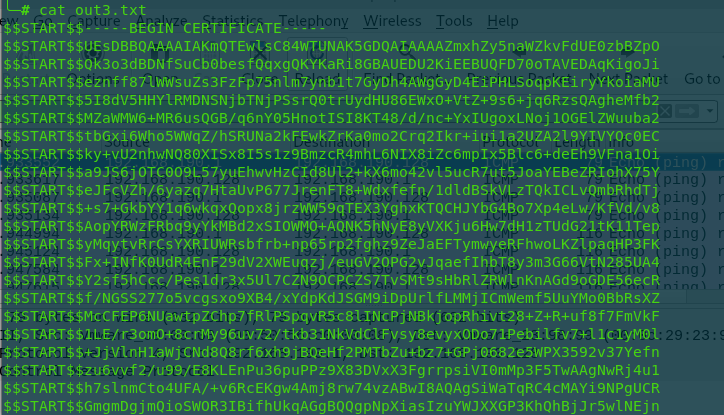


Hex解码

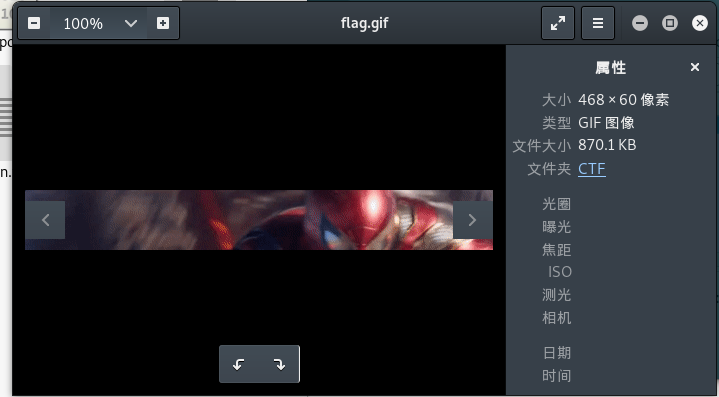


发现重复的，语句

使用uniq 文件路径去重

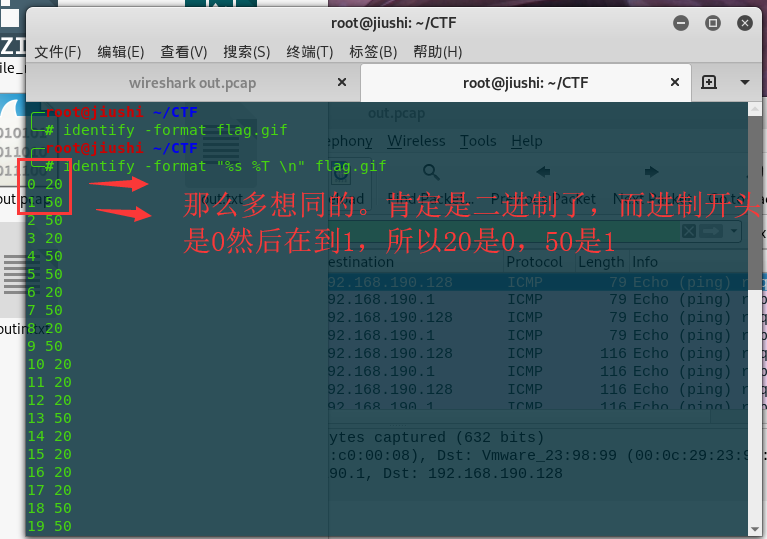


用py解码Base64，得到一个压缩包，解压之后是个flag.gif



获取帧之间的时间间隔

identify -format "%s %T \n" flag.gif



二进制转字符串后，得到

mD5\_1t

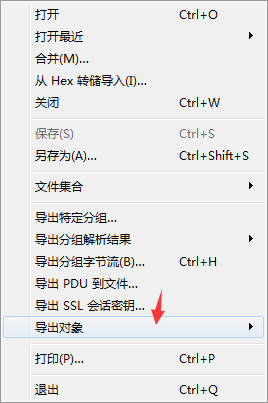
根据题目提示进行md5加密，将md5\_32位小写的交上去即可



参考文章：<https://www.cnblogs.com/ls-pankong/p/8944584.html>

数据包做题常规思路：

1.先通过导出对象来分析HTTP



3.如果发现HTTP只有一个请求的话，说明这道题的关键不在http流量里，此时应该去找别的协议观察看看

4.在观察流量的时候发现flag关键字的话，跟着这部走。如果出现提示什么压缩包之类的东西或者说要密码才能得到flag，flag.txt的。但是流量里面又没文件数据的话，binwalk 数据包，一般都能得到隐藏文件（配合Ctrl+F搜索）

5.发现一些类似于图片的特征的话，先把图片保存下来。如图片的十六进制开头是FF D8

