




# BUUCTF: greatescape

原创

末初  于 2020-08-02 16:46:28 发布  767  收藏 2

分类专栏: [CTF\\_MISC\\_Writeup](#) 文章标签: [BUUCTF greatescape](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/mochu7777777/article/details/107743870>

版权



[CTF\\_MISC\\_Writeup](#) 专栏收录该内容

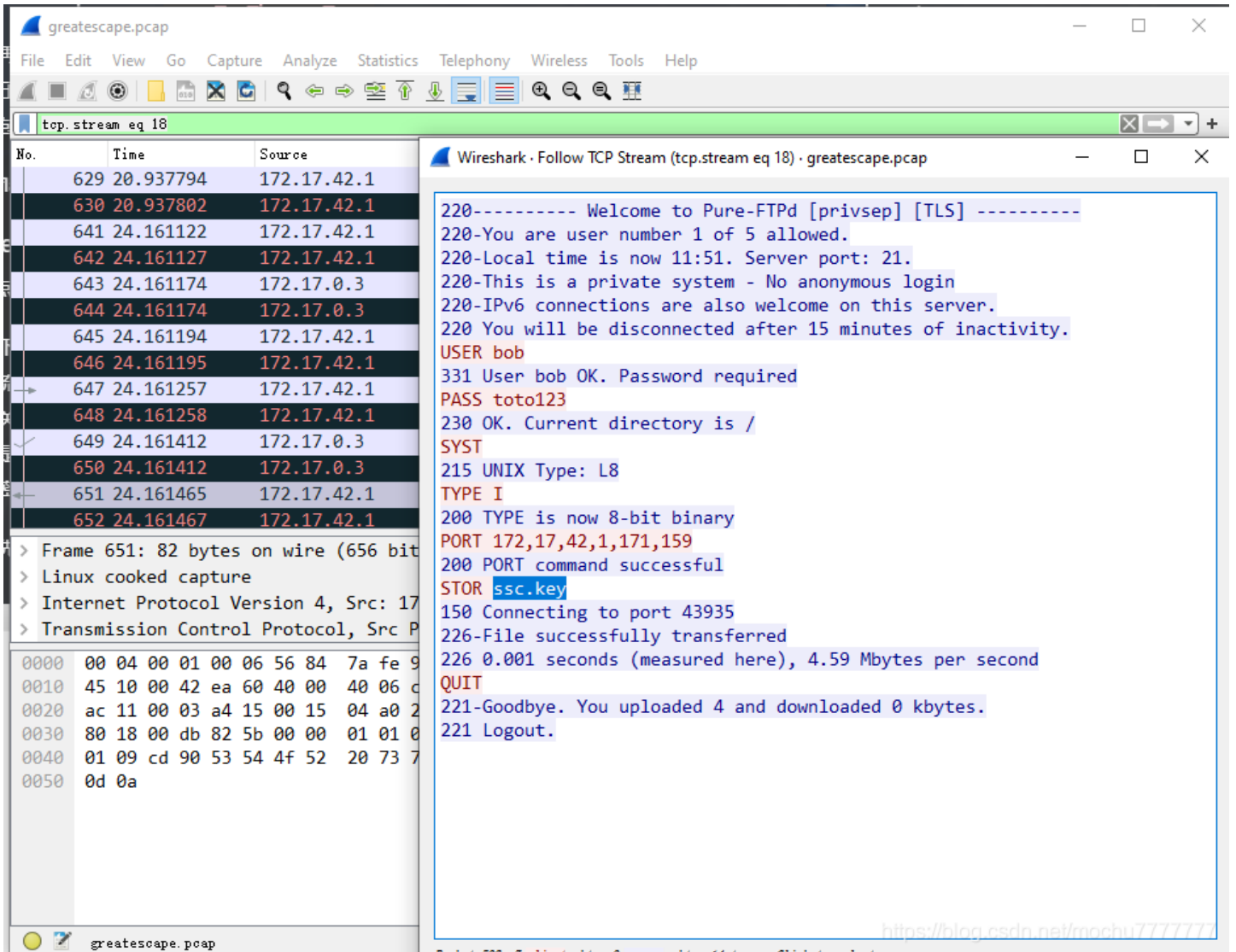
246 篇文章 45 订阅

订阅专栏

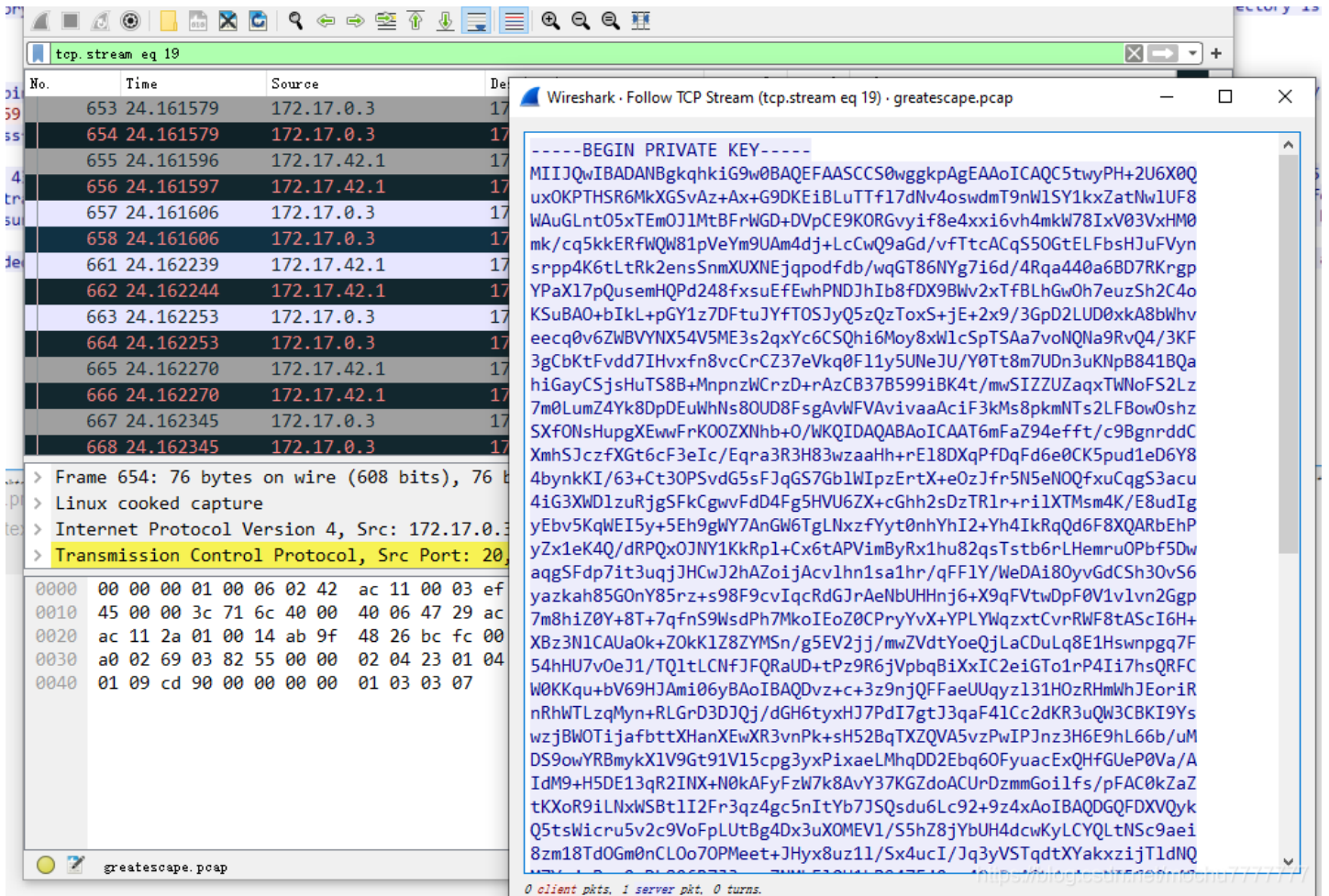
题目地址: <https://buuoj.cn/challenges#greatescape>



下载附件得到一个流量包，追中 TCP 流，在 tcp.stream eq 18，发现 ssc.key



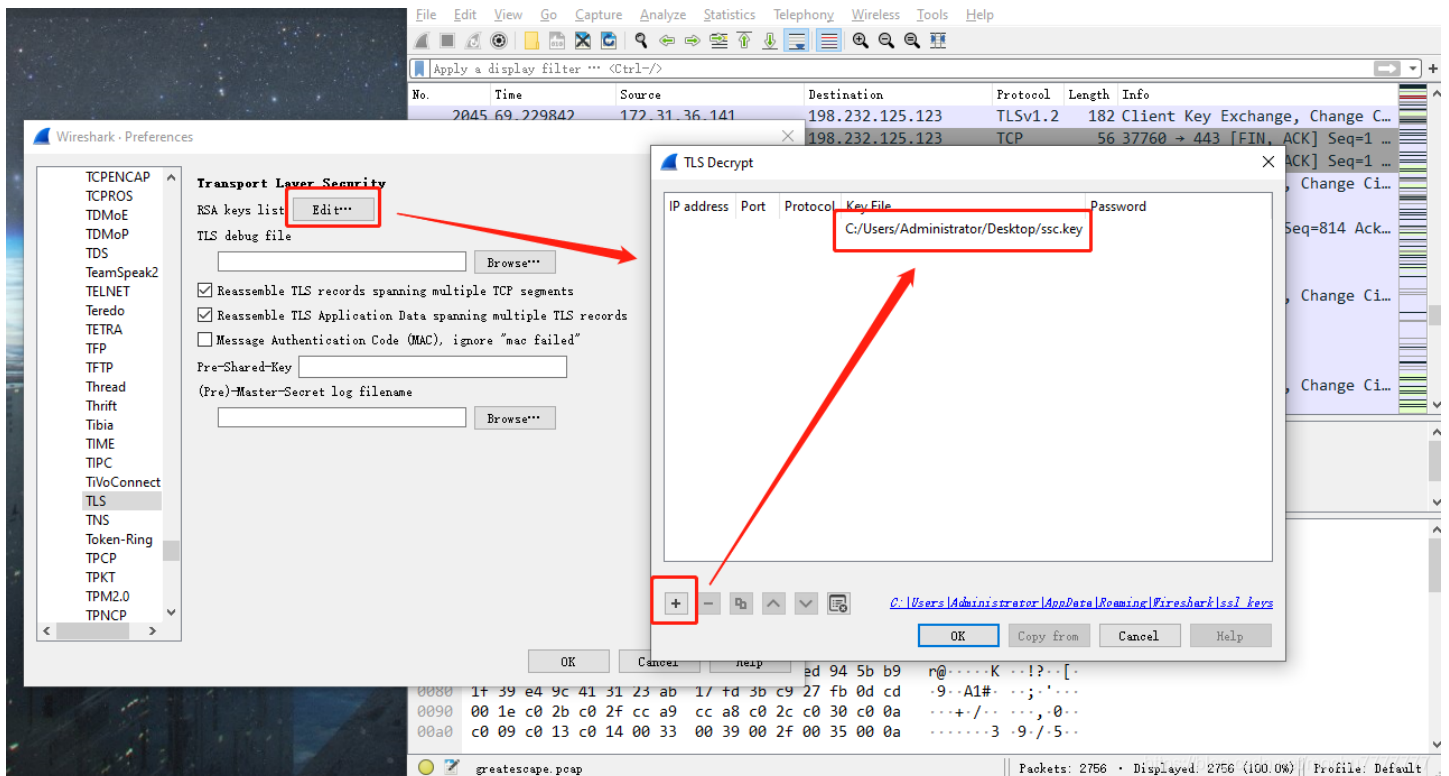
在 tcp.stream eq 19 看到 rsa 私钥格式的key



将私钥先保存下来名为 `ssc.key`

通过分析流量猜测，这应该在向 `ftp` 服务器传送私钥，我们得到了私钥，就可以解密 `TLS` 报文

`Edit->Preference->Protocols->TLS`，点击 `Edit`，然后点击 `+` 添加 `Key File`



然后在 tcp.stream eq 80 追踪 TLS Stream 即可发现flag

The screenshot shows the Wireshark interface with a packet capture named 'greescape.pcap'. The main pane displays a list of packets, with packet 2206 selected. The details pane shows the following information:

- Content-Length: 3
- Keep-Alive: timeout=5, max=96
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8
- GET /api/files.php?action=list HTTP/1.1
- Host: ssc.teaser.insomnihack.ch
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:50.0) Gecko/20100101 Firefox/50.0
- Accept: application/json, text/plain, \*/\*
- Accept-Language: en-US,en;q=0.5
- Accept-Encoding: gzip, deflate, br
- Referer: https://ssc.teaser.insomnihack.ch/files
- Cookie: PHPSESSID=3u5dqmfudc7ap1di0nmfjgtjm3
- FLAG: INS{OkThatWasWay2Easy}** (highlighted with a red box)
- Connection: keep-alive
- HTTP/1.1 200 OK
- Date: Fri, 20 Jan 2017 11:52:07 GMT
- Server: Apache
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Cache-Control: no-store, no-cache, must-revalidate
- Pragma: no-cache
- Content-Length: 3
- Keep-Alive: timeout=5, max=95
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8

The packet bytes pane shows the raw data for the selected packet, and the packet list pane shows the details of the selected packet.

flag{OkThatWasWay2Easy}