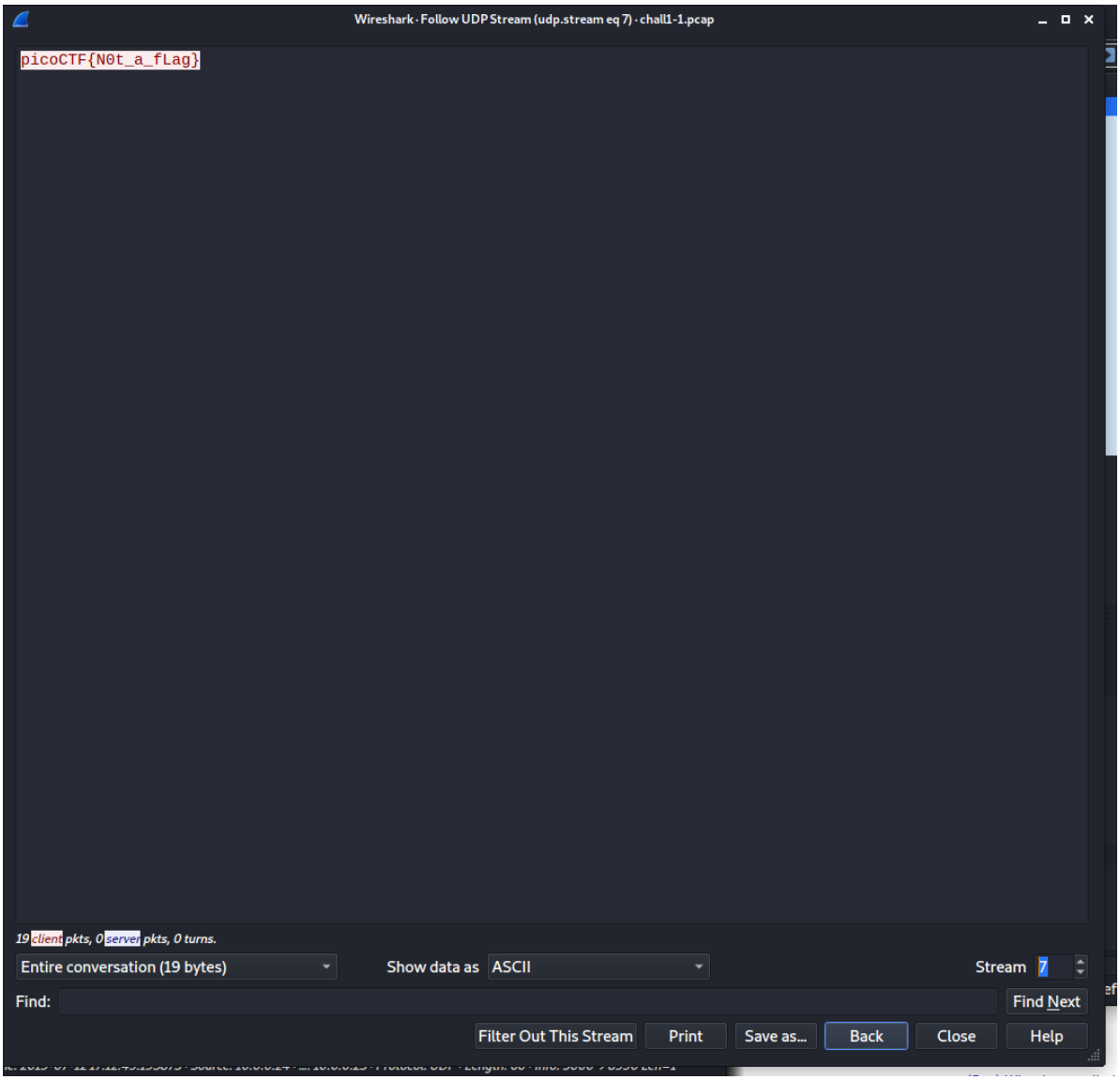
Lab1 CTF Writeup

孙永康　11911409

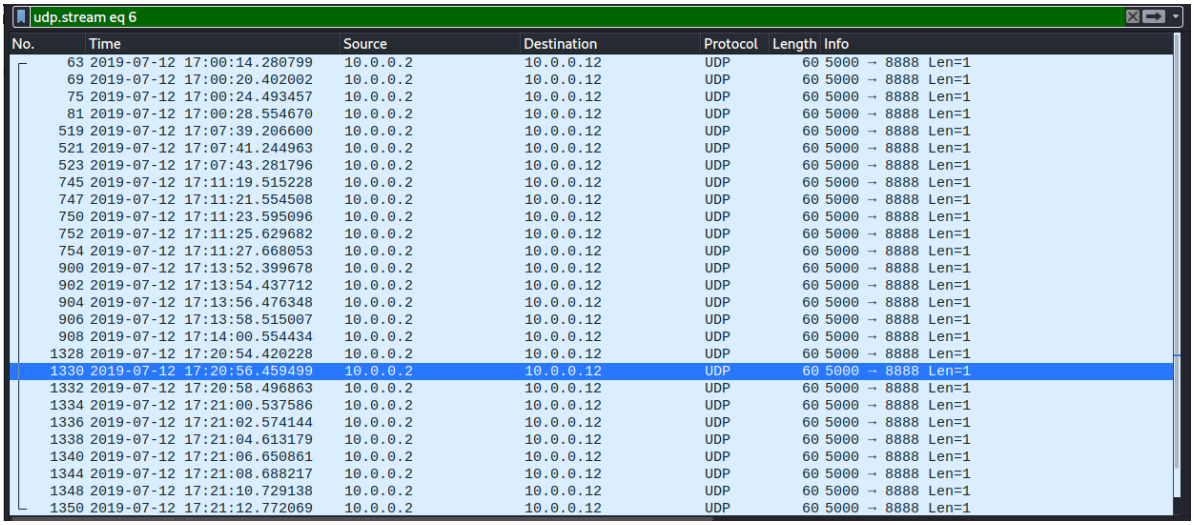
Question 1 :

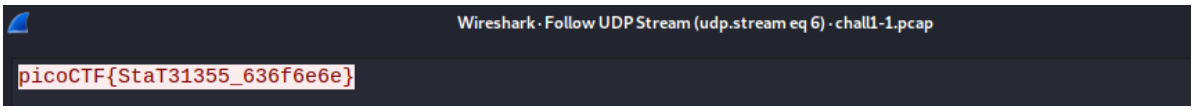
This question give me some hint of "UDP" and "streams", so I try to follow those streams in wireshark.

then I find a "not a flag", but I realize that I can change the button of "stream" at the right bottom to quickly check all the other steams with different number.



and then I find this one when I change the stream number to 6:





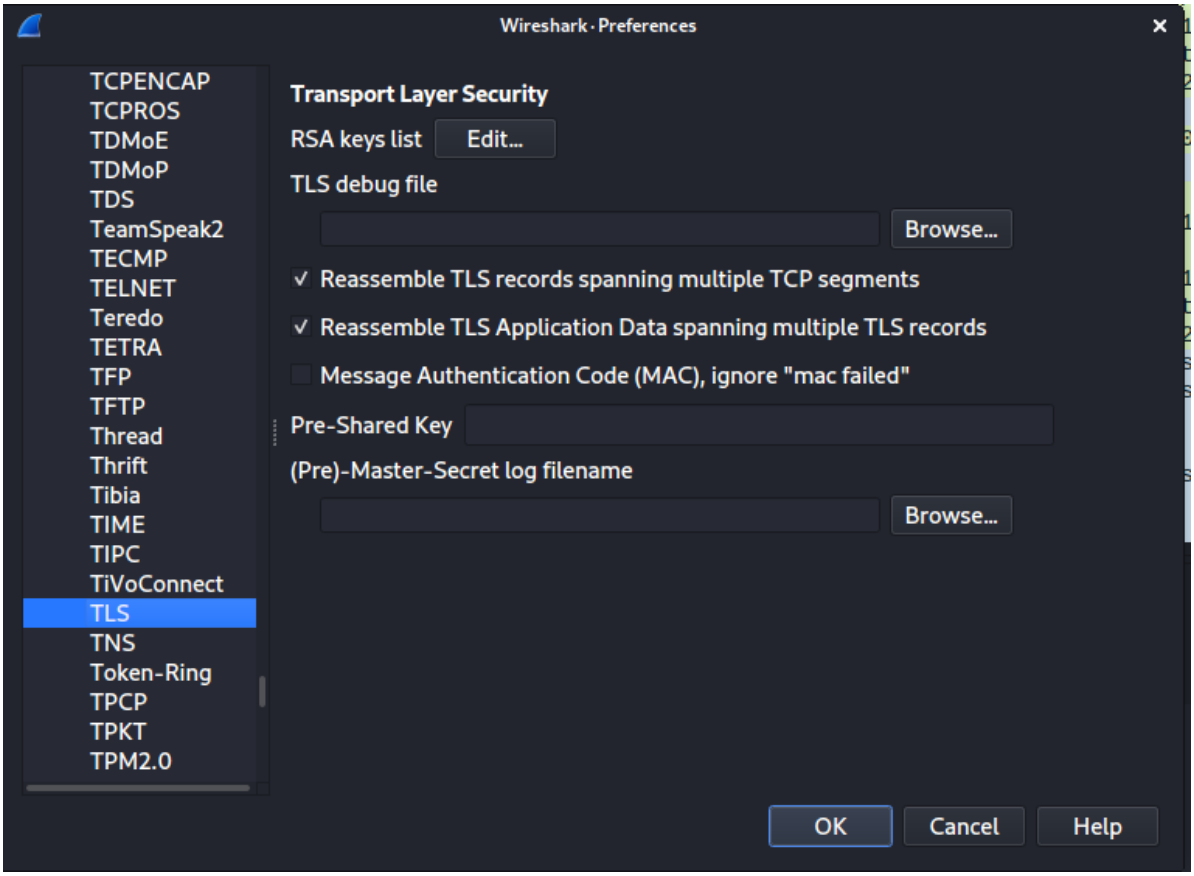
The flag I found is **picoCTF{StaT31355_636f6e6e}**

Question 2 :

This problem give us 2 files, first one which can be opened in wireshark maybe contains the HTTP pack and we can found flags in it. Second one is a log file which indicates that it is used in SSL/TSL protocols.

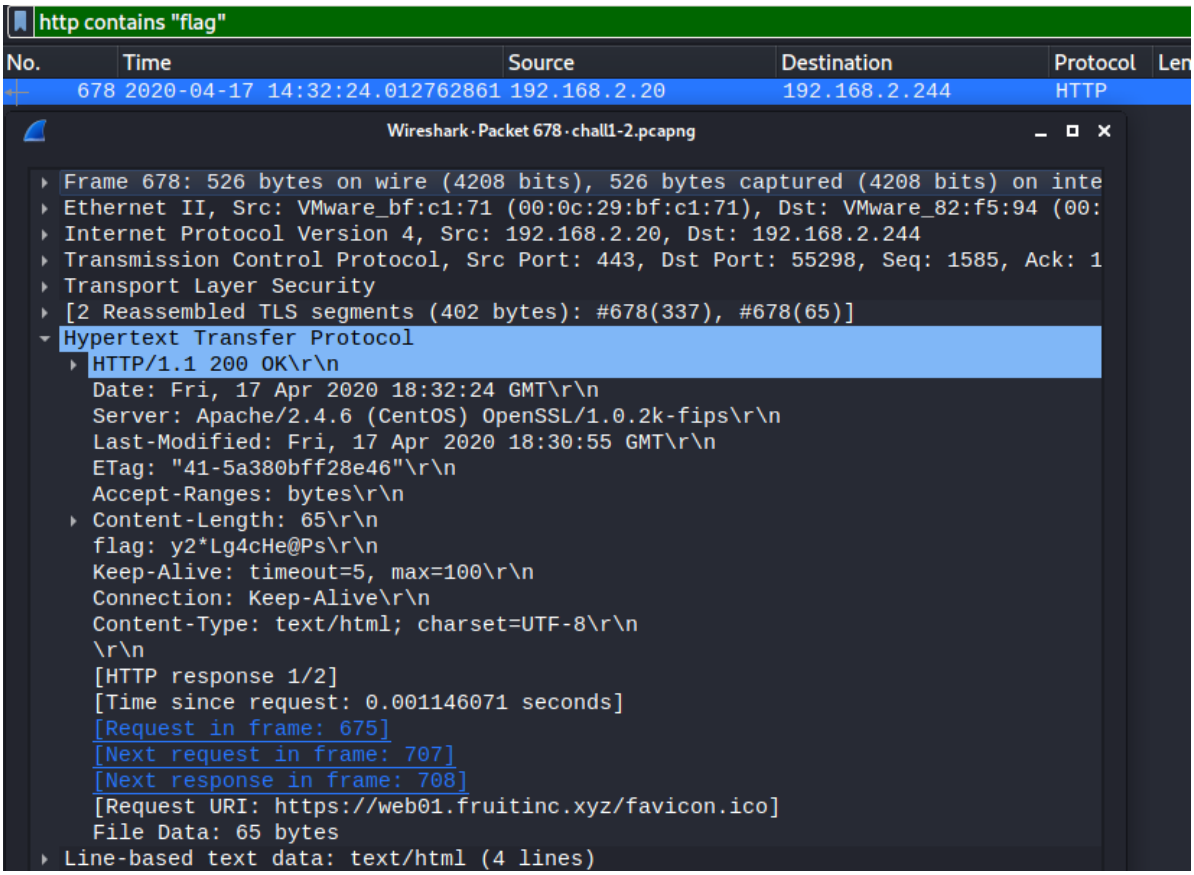
```
# SSL/TLS secrets log file, generated by NSS
CLIENT_RANDOM 1a70cc96e200ad78a1073ab963a6f2683c042cfa76a21e43205adba8d9b56303 62b6c6b6b57d771821e1561e48aec5b1ce4d6f5a109dcd81dd6ce15c7db58aace1c4fe2fb555d85b504846b80e69a9bd
CLIENT_RANDOM 00ba831f948c5a436bccae8ef0050c5327011cf36a29e50927717e67e07e788d 62b6c6b6b57d771821e1561e48aec5b1ce4d6f5a109dcd81dd6ce15c7db58aace1c4fe2fb555d85b504846b80e69a9bd
CLIENT_RANDOM fa0f244a1775672d8850613a1ed5161ad55b1fac2d4413385b3b446a51700ad0 6445e58e12ae0e2c192532d15f0797af3687fee17d45da46aa28798833e8abd4998784329ab143aead37d4d1cf5b5166
CLIENT_RANDOM 92ac4876d712c9e29c5afc9e4993cf3c886c1c52ee22f7971547073e57af4046 bcd154c38b38e9deaa0d9a5945ed7899c17debdafe6dbcac3b3d5454e7d5ef54de829fecdc1862b5c4239b628af1b1f1
CLIENT_RANDOM 797e5f939fe5dc4b950175d6fd8772b0323bd8b805dc6ebe1cd62f195e452295 bcd154c38b38e9deaa0d9a5945ed7899c17debdafe6dbcac3b3d5454e7d5ef54de829fecdc1862b5c4239b628af1b1f1
CLIENT_RANDOM 912e7c0714f58b1af3f2f79a25209b0237139b77304b1bdd741c91eca854b470 3b92def832a4857278a9953f641af0eb07af8bfabd0c69da2d54885d0c21c1610d2193be10810f2398ec5dd65dd96bdb
CLIENT_RANDOM d88d465d39fe2ee9e6dba9494a2d0f6ac798a9419efb83fa86d6ae7b11061284 24c99f00d69610b31595d7c0f1f2d1cb376354f2e40cf449264beb386a1f88e8c0ea7a3b148845b30e79cb04046dd413
CLIENT_HANDSHAKE_TRAFFIC_SECRET 03312834e5df543433caa03f6b409360f7cc70ae35b58a886536c4a2399c9c82
8b6a2c5cb6a9be3356f1add9d08d869f674cfbaae143a1c627c8b129c704e00e38ce0ceb73861bffdc0f2135fa74b964
SERVER_HANDSHAKE_TRAFFIC_SECRET 03312834e5df543433caa03f6b409360f7cc70ae35b58a886536c4a2399c9c82
a3baleee0122bca9e03b8a32e8e14e993d7ea3d869c5b2f0c8c60816fbd2d362d7eccf0133b920f3c72bce2411b3dd67
CLIENT_HANDSHAKE_TRAFFIC_SECRET cb8b936b9fbcf8e57eebcf57e40eb748519356dfa39c43d8b4c16a46f338d760
```

After searching some information on internet, I notice that SSL/TSL is used by HTTP protocols to encrypt its message. So, searching more information about how to use wireshark to decrypt these kind of decryptions. Then I found this article[[https][tls] 如何使用wireshark查看tls/https加密消息--使用keylog - toong - 博客园 (cnblogs.com)]. Follow the instructions of the articles, I put log file into the wireshark:



The block in the bottom is used to put in blog file. However I can not fully acknowledge what these settings all about, I think I may do some further research later.

However, After putting it in, everything become better. Easily filter with "http contains "flag"" , I found the only one left which absolutely contains the flag.



So, the flag is **flag{y2*Lg4cHe@Ps}**