

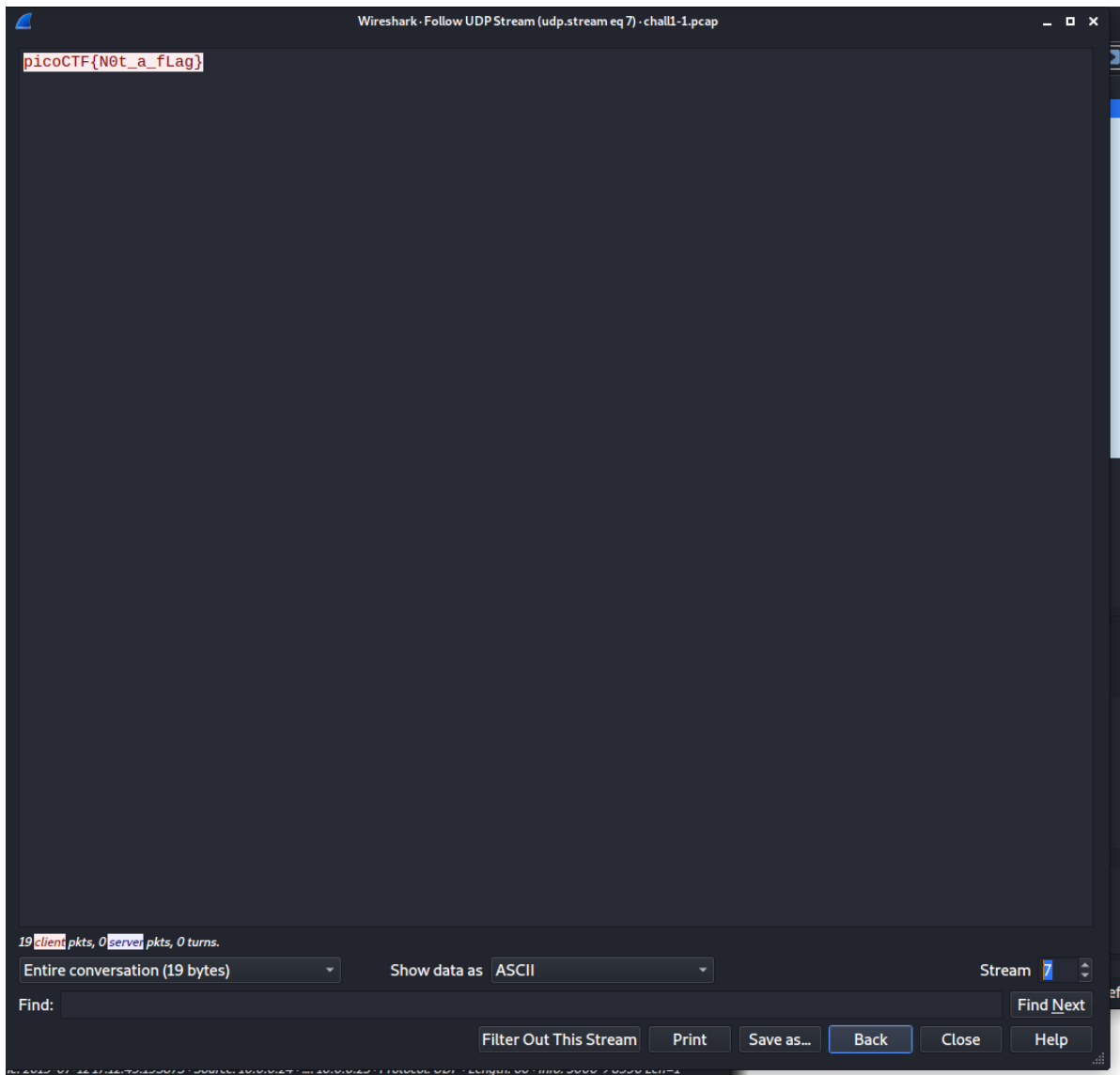
Lab1 CTF Writeup

孙永康 11911409

Question 1 :

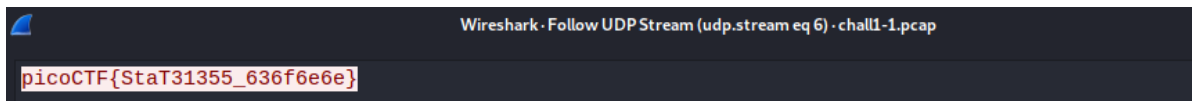
This question give me some hint of "UDP" and "streams", so I try to follow those streams in wireshark.

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 steams with different number.



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

No.	Time	Source	Destination	Protocol	Length	Info
63	2019-07-12 17:00:14.280799	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
69	2019-07-12 17:00:20.402002	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
75	2019-07-12 17:00:24.493457	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
81	2019-07-12 17:00:28.554670	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
519	2019-07-12 17:07:39.206600	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
521	2019-07-12 17:07:41.244963	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
523	2019-07-12 17:07:43.281796	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
745	2019-07-12 17:11:19.515228	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
747	2019-07-12 17:11:21.554508	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
750	2019-07-12 17:11:23.595096	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
752	2019-07-12 17:11:25.629682	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
754	2019-07-12 17:11:27.668053	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
900	2019-07-12 17:13:52.399678	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
902	2019-07-12 17:13:54.437712	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
904	2019-07-12 17:13:56.476348	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
906	2019-07-12 17:13:58.515007	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
908	2019-07-12 17:14:00.554434	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1328	2019-07-12 17:20:54.420228	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1330	2019-07-12 17:20:56.459499	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1332	2019-07-12 17:20:58.496863	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1334	2019-07-12 17:21:00.537586	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1336	2019-07-12 17:21:02.574144	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1338	2019-07-12 17:21:04.613179	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1340	2019-07-12 17:21:06.650861	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1344	2019-07-12 17:21:08.688217	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1348	2019-07-12 17:21:10.729138	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1
1350	2019-07-12 17:21:12.772069	10.0.0.2	10.0.0.12	UDP	60	5000 → 8888 Len=1



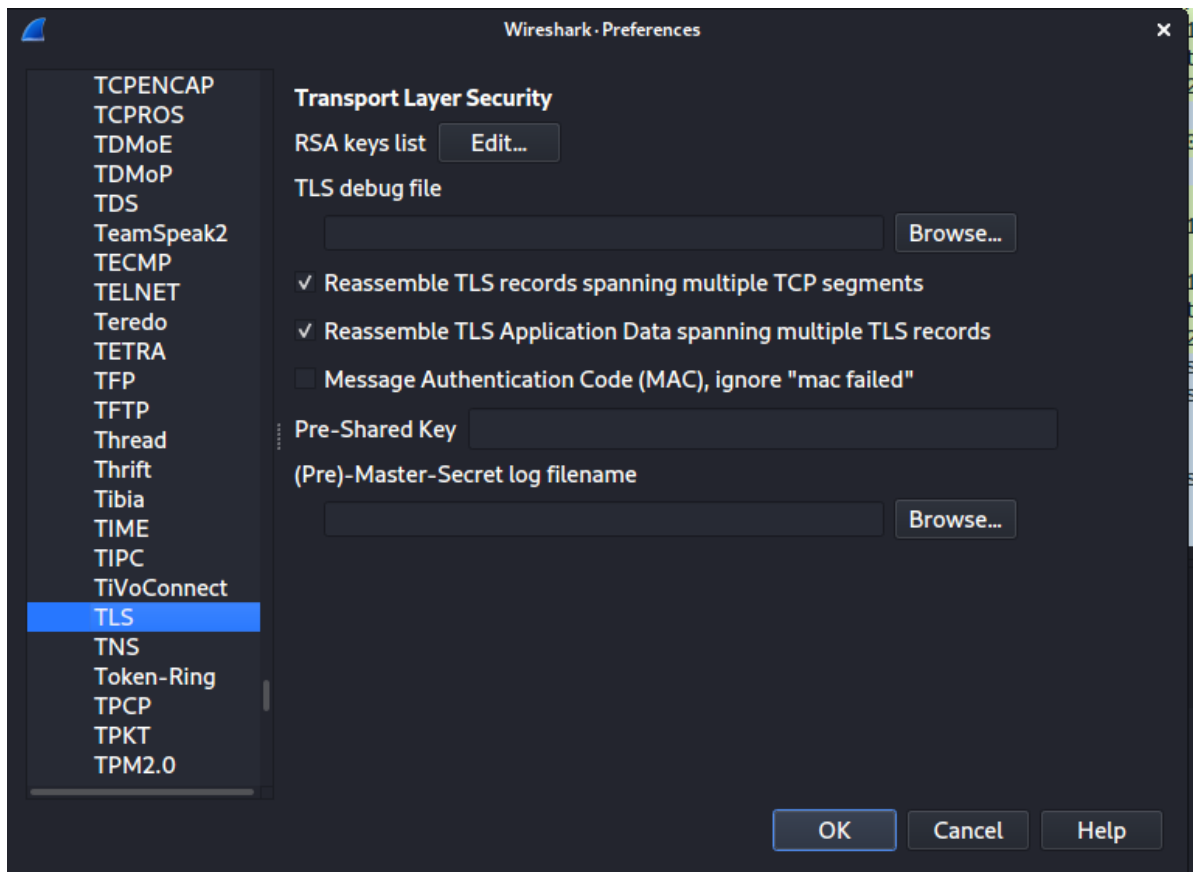
The flag I found is **picoCTF{StaT31355_636f6e6e}**

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.

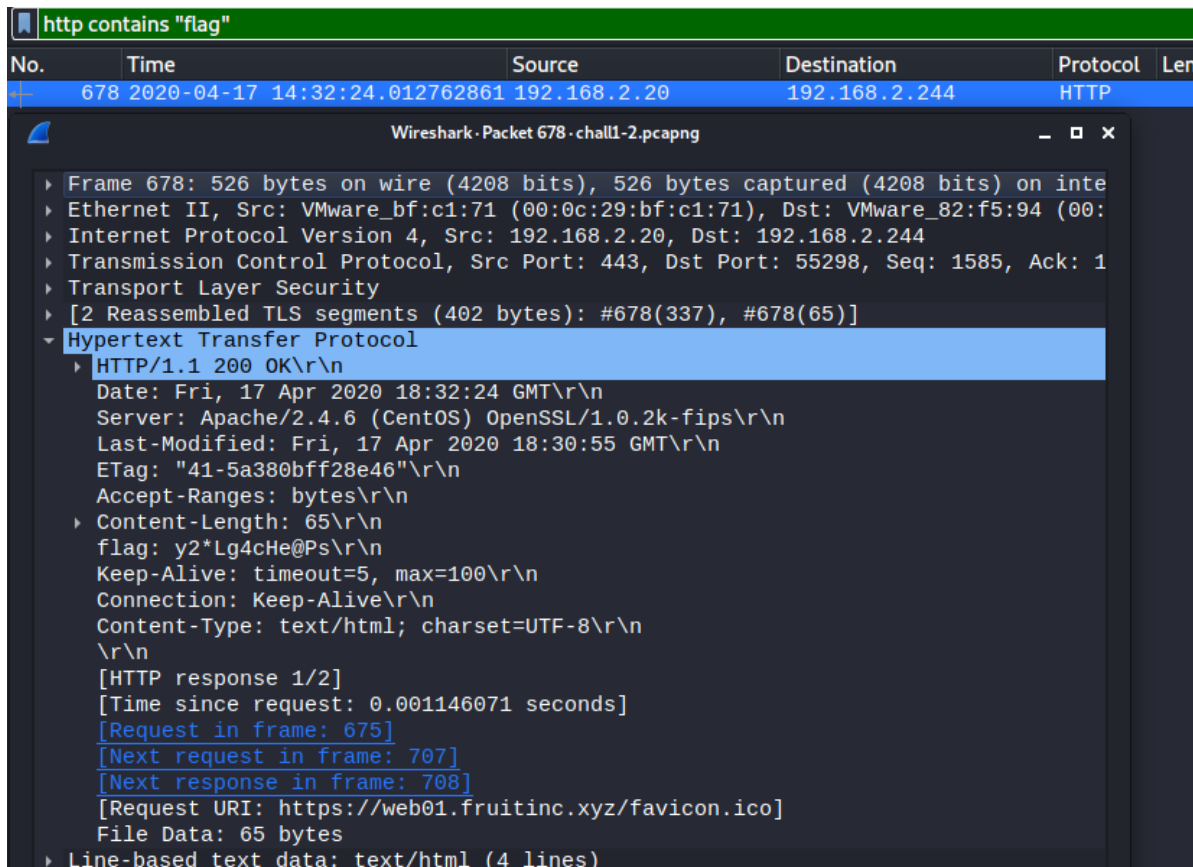
```
# SSL/TLS secrets log file, generated by NSS
CLIENT_RANDOM 1a70cc9e200ad78a1073ab963a6f2683c042cfa76a21e43205adba8d9b56303 62b6c6b6b57d771821e1561e48a5b1ce4d6f5a109dc081dd6ce15c7db58aace1c4fe2fb555d85b504846b80e69a9bd
CLIENT_RANDOM 00ba831f948c5a436bcca8e0f0050c5327011cf36a29e50927717e67e07e7880 62b6c6b6b57d771821e1561e48a5b1ce4d6f5a109dc081dd6ce15c7db58aace1c4fe2fb555d85b504846b80e69a9bd
CLIENT_RANDOM fa0f244a1775672d8050613a1eds16ad55b1fac2d4413385b3b446a517809d0 6445e58e12ae0e2c192532d15f0797af3687fee17d45da46aa20798833e8ab04998784329ab143aeadd3704d1cf5b5166
CLIENT_RANDOM 92ac4876d712c9e29c5afce94993cf3c886c1c52ee2f7971547073e57af4046 bcd154c38b38e9dea0d9a5945ed7899c17debdafe8dbcac3b3d5454e7d5ef54de829fecdc1862b5c4239b628af1b1f1
CLIENT_RANDOM 797a5f939fe5dc4b950175d6f872b0323bd8b805dc6ebe1cd62f195e452295 bcd154c38b38e9dea0d9a5945ed7899c17debdafe8dbcac3b3d5454e7d5ef54de829fecdc1862b5c4239b628af1b1f1
CLIENT_RANDOM 912e7c0714f58b1af3f2f79a25209b0237139b77304b1bdd741c91eca854b470 3b92def832a4857278a9953f641af0eb07af8bfabddc69da2d54885d0c21c1610d2193be10810f2398ec5dd5dd96bdb
CLIENT_RANDOM d88d465d39fe2ee9e6dba9494a2d0f6ac798a9419efb83fa86d6ae7b11061284 24c99f00d69610b31595d7c0f1f2d1cb376354f2e40cf449264deb386a1f88e8c0ea7a3b148845b30e79cb04046d4d13
CLIENT_HANDSHAKE_TRAFFIC_SECRET 03312834e5df543433caa03f6b409360f7cc70ae35b58a886536c4a2399c9c82
8b6a2c5cbb9a9e3556f1add9d08d869f674cfbaae143a1c627c8b129c704e00e38ce0bcb73861bffdcbf2135fa74b964
SERVER_HANDSHAKE_TRAFFIC_SECRET 03312834e5df543433caa03f6b409360f7cc70ae35b58a886536c4a2399c9c82
a3ba1ee0122bca9e03b8a32e8e14e993d7ea3d869c5b2f0c8c60816fbd2d362d7eccf0133b920f3c72bce2411b3d6d7
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://cnblogs.com/toong/p/1111111.html>]]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}**

