CTF省赛练习笔记（1）流量分析WP

原创

JaySRJ7 于 2019-10-06 10:42:25 发布 1590 收藏 1

文章标签： CTF练习

本文链接：https://blog.csdn.net/JaySRJ7/article/details/102215248

**

CTF省赛练习笔记MISC—流量分析篇

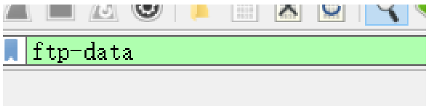
**

一、第三届上海市网络安全大赛

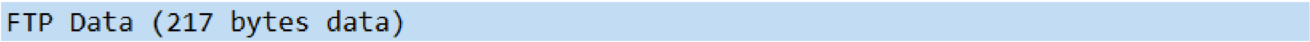
流量分析——traffic

1.下载附件用wireshark打开

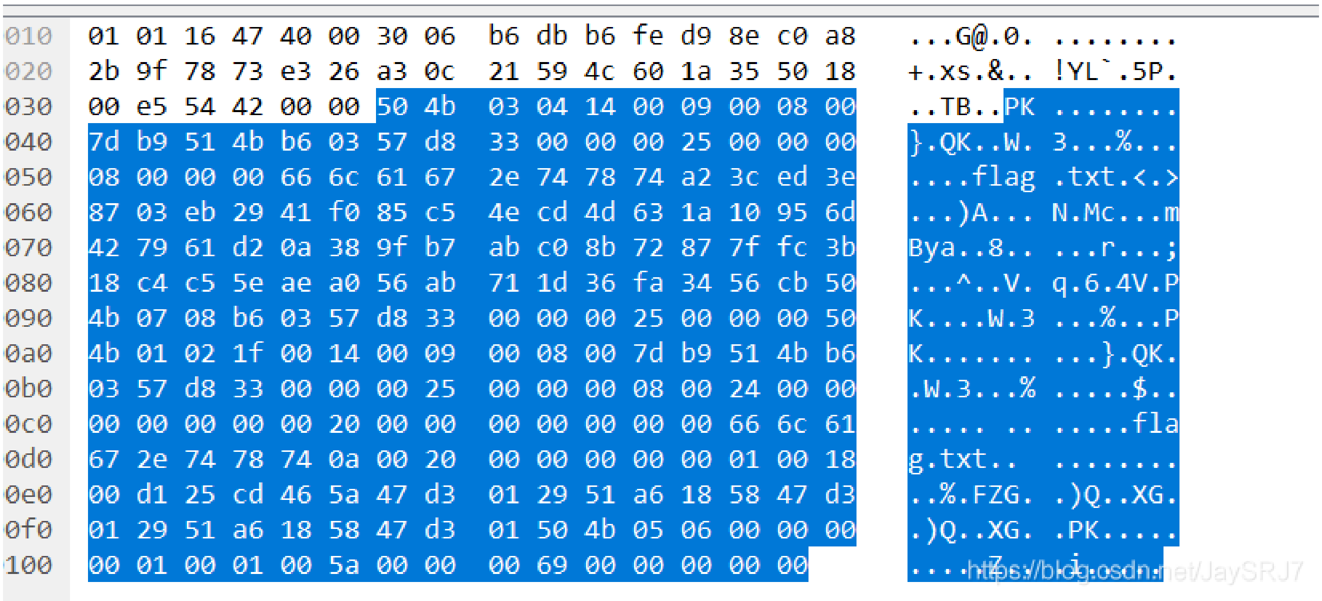
2.一开始搜索字符串flag没有发现什么有价值的东西，接下来想到筛选一些流量进行分析，在筛选ftp-data时发现有几条流量都含有flag.zip，想到将他们导出分组字节流。



```
ftp-data
```

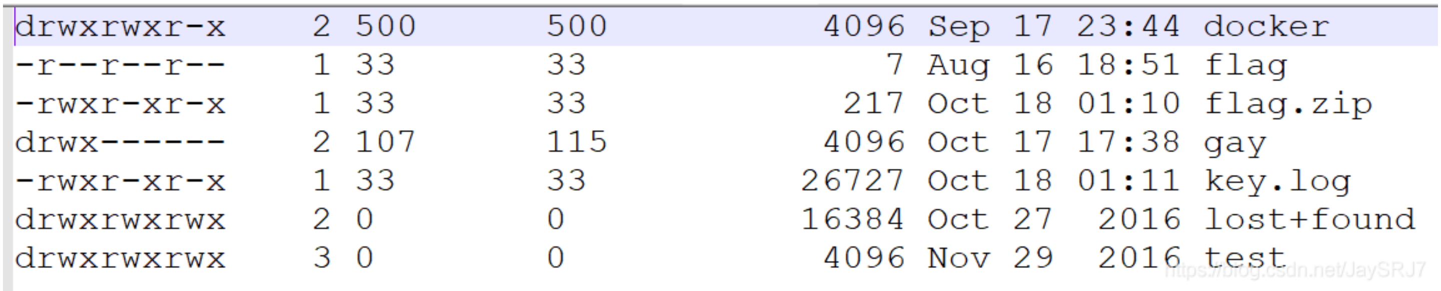


```
FTP Data (217 bytes data)
```

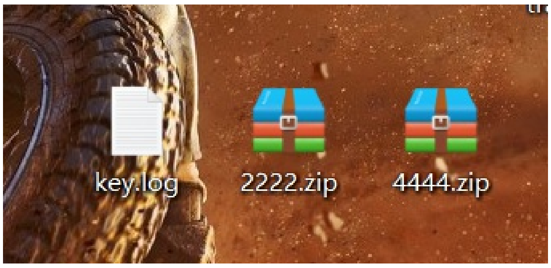


```
010  01 01 16 47 40 00 30 06  b6 db b6 fe d9 8e c0 a8   ...G@.0. ........
020  2b 9f 78 73 e3 26 a3 0c  21 59 4c 60 1a 35 50 18   +.xs.&.. !YL`.5P.
030  00 e5 54 42 00 00 50 4b  03 04 14 00 09 00 08 00   ..TB..PK ........
040  7d b9 51 4b b6 03 57 d8  33 00 00 00 25 00 00 00   }.QK..W. 3...%...
050  08 00 00 00 66 6c 61 67  2e 74 78 74 a2 3c ed 3e   ....flag .txt.<.>
060  87 03 eb 29 41 f0 85 c5  4e cd 4d 63 1a 10 95 6d   ...)A... N.Mc...m
070  42 79 61 d2 0a 38 9f b7  ab c0 8b 72 87 7f fc 3b   Bya..8.. ...r...;
080  18 c4 c5 5e ae a0 56 ab  71 1d 36 fa 34 56 cb 50   ...^..V. q.6.4V.P
090  4b 07 08 b6 03 57 d8 33  00 00 00 25 00 00 00 50   K....W.3 ...%...P
0a0  4b 01 02 1f 00 14 00 09  00 08 00 7d b9 51 4b b6   K....... ...}.QK.
0b0  03 57 d8 33 00 00 00 25  00 00 00 08 00 24 00 00   .W.3...% .....$..
0c0  00 00 00 00 00 20 00 00  00 00 00 00 00 66 6c 61   ..... .. .....fla
0d0  67 2e 74 78 74 0a 00 20  00 00 00 00 00 01 00 18   g.txt.. ........
0e0  00 d1 25 cd 46 5a 47 d3  01 29 51 a6 18 58 47 d3   ..%.FZG. .)Q..XG.
0f0  01 29 51 a6 18 58 47 d3  01 50 4b 05 06 00 00 00   .)Q..XG. .PK.....
100  00 01 00 01 00 5a 00 00  00 69 00 00 00 00 00      .....Z.. .i.....
```

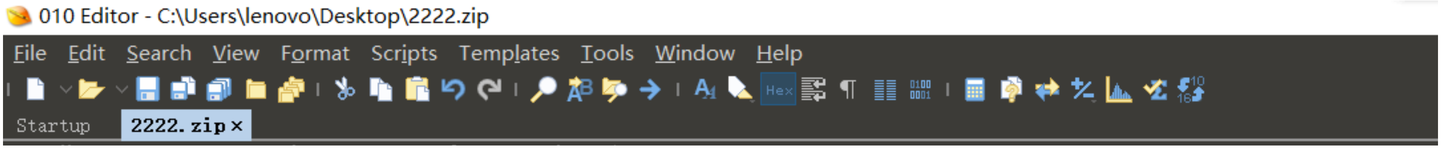
3.经过分析后发现可以导出的是一个key.log和两个压缩包（key.log能发现这是一份NSS Key Log Format的文件，而这个文件是能解密出 Wireshark 里面的 https 流量的）

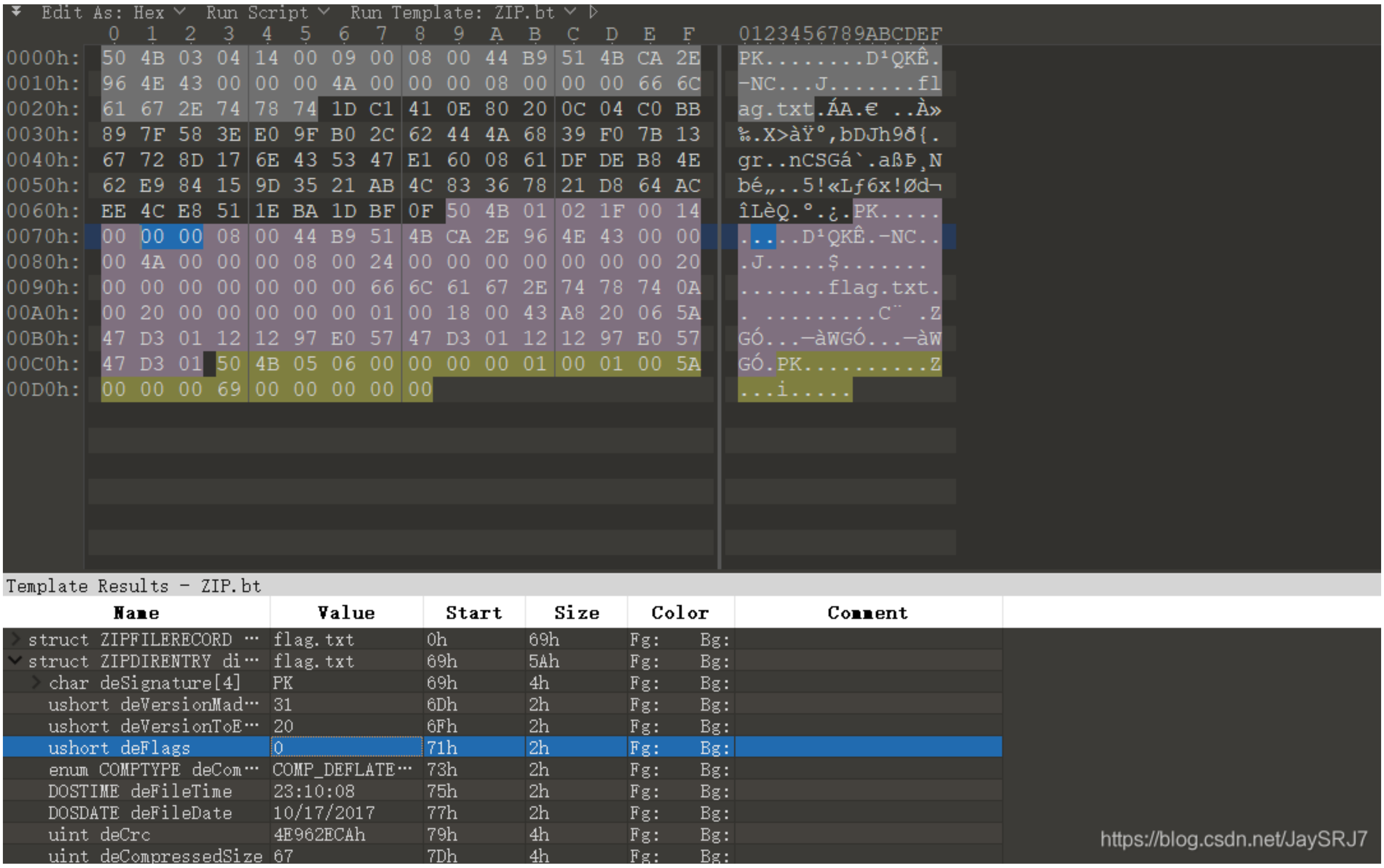


```
drwxrwxr-x    2 500      500          4096 Sep 17 23:44 docker
-r--r--r--    1 33       33              7 Aug 16 18:51 flag
-rwxr-xr-x    1 33       33            217 Oct 18 01:10 flag.zip
drwx------    2 107      115          4096 Oct 17 17:38 gay
-rwxr-xr-x    1 33       33          26727 Oct 18 01:11 key.log
drwxrwxrwx    2 0        0           16384 Oct 27  2016 lost+found
drwxrwxrwx    3 0        0            4096 Nov 29  2016 test
```



4.查看一下压缩包中的内容发现都是经过加密的flag.txt文件，暴力破解无法解决后想到了伪加密的方法，于是用010edito进行破解，将value由9改为0，结果发现一个是伪加密而另一个不是。


010 Editor - C:\Users\lenovo\Desktop\2222.zip
File Edit Search View Format Scripts Templates Tools Window Help
Hex
Startup
2222.zip ×

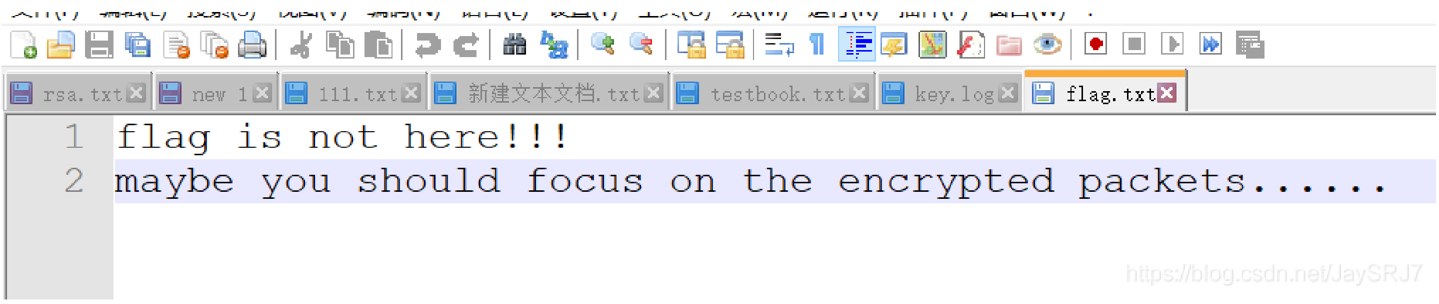


```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 50 4B 03 04 14 00 09 00 08 00 44 B9 51 4B CA 2E   PK........D¹QKÊ.
0010h: 96 4E 43 00 00 00 4A 00 00 00 08 00 00 00 66 6C   –NC...J.......fl
0020h: 61 67 2E 74 78 74 1D C1 41 0E 80 20 0C 04 C0 BB   ag.txt.ÁA.€ ..À»
0030h: 89 7F 58 3E E0 9F B0 2C 62 44 4A 68 39 F0 7B 13   ‰.X>àŸ°,bDJh9ð{.
0040h: 67 72 8D 17 6E 43 53 47 E1 60 08 61 DF DE B8 4E   gr..nCSGá`.aßÞ¸N
0050h: 62 E9 84 15 9D 35 21 AB 4C 83 36 78 21 D8 64 AC   bé„..5!«Lƒ6x!Ød¬
0060h: EE 4C E8 51 1E BA 1D BF 0F 50 4B 01 02 1F 00 14   îLèQ.º.¿.PK.....
0070h: 00 00 00 08 00 44 B9 51 4B CA 2E 96 4E 43 00 00   .....D¹QKÊ.–NC..
0080h: 00 4A 00 00 00 08 00 24 00 00 00 00 00 00 00 20   .J.....$.......
0090h: 00 00 00 00 00 00 00 66 6C 61 67 2E 74 78 74 0A   .......flag.txt.
00A0h: 00 20 00 00 00 00 00 01 00 18 00 43 A8 20 06 5A   . .........C¨ .Z
00B0h: 47 D3 01 12 12 97 E0 57 47 D3 01 12 12 97 E0 57   GÓ...—àWGÓ...—àW
00C0h: 47 D3 01 50 4B 05 06 00 00 00 00 01 00 01 00 5A   GÓ.PK..........Z
00D0h: 00 00 00 69 00 00 00 00 00                        ...i.....
```

Template Results - ZIP.bt

Name	Value	Start	Size	Color		Comment
struct ZIPFILERECORD ···	flag.txt	0h	69h	Fg:	Bg:	
struct ZIPDIRENTRY di···	flag.txt	69h	5Ah	Fg:	Bg:	
char deSignature[4]	PK	69h	4h	Fg:	Bg:	
ushort deVersionMad···	31	6Dh	2h	Fg:	Bg:	
ushort deVersionToE···	20	6Fh	2h	Fg:	Bg:	
ushort deFlags	0	71h	2h	Fg:	Bg:	
enum COMPTYPE deCom···	COMP_DEFLATE···	73h	2h	Fg:	Bg:	
DOSTIME deFileTime	23:10:08	75h	2h	Fg:	Bg:	
DOSDATE deFileDate	10/17/2017	77h	2h	Fg:	Bg:	
uint deCrc	4E962ECAh	79h	4h	Fg:	Bg:	
uint deCompressedSize	67	7Dh	4h	Fg:	Bg:	

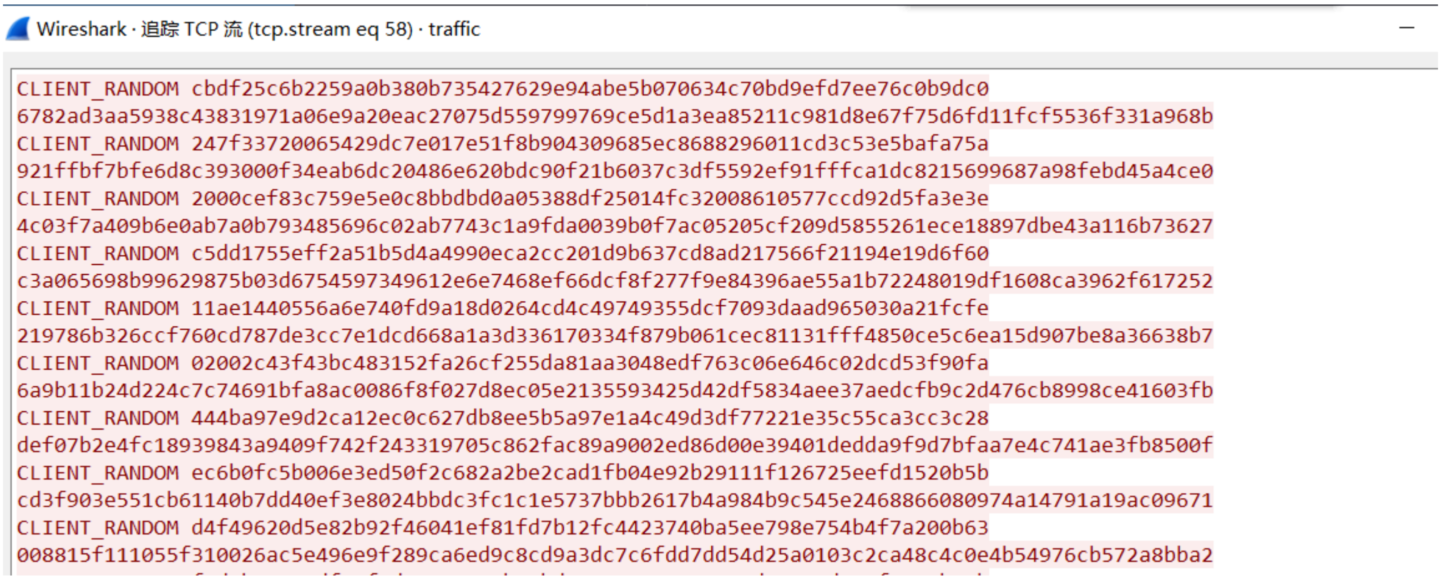
5.打开这个文档发现flag竟然是假的。。。好吧，我就知道没有这么简单，但是通过这个提示我们可以知道这个流量包是被加密过的，综合上面得到的key.log不难知道要得到真正的flag需要对这个流量包进行解密



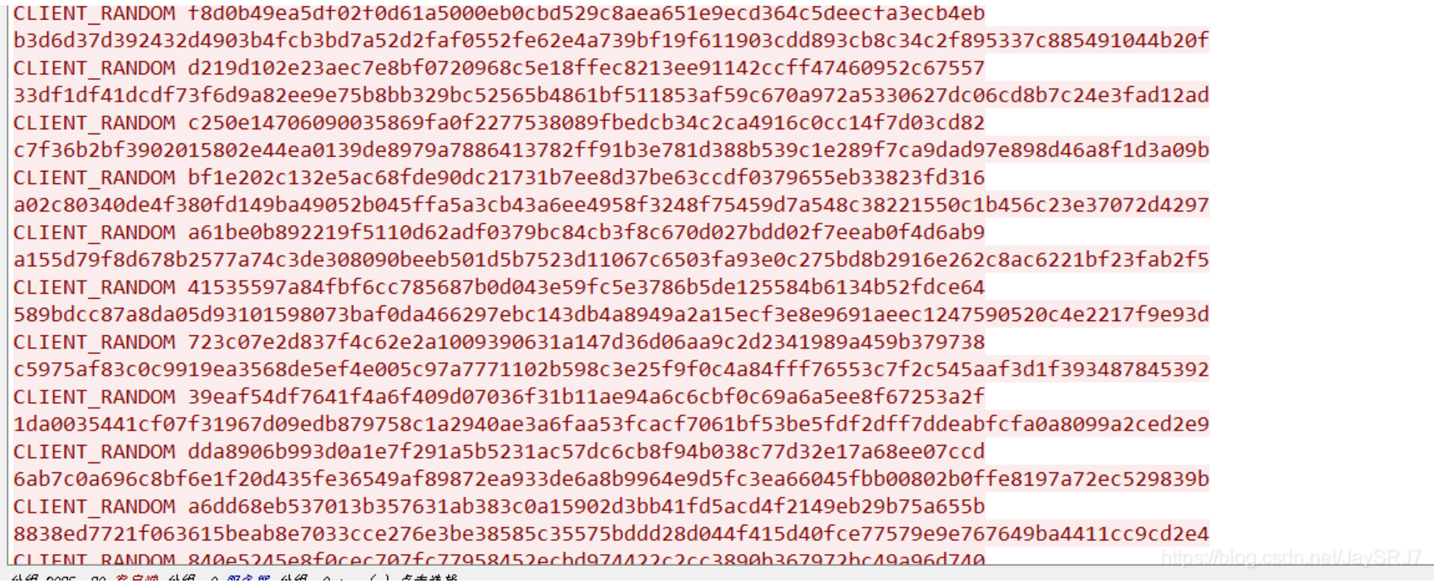
```
flag is not here!!!
maybe you should focus on the encrypted packets......
```

6.虽然没有得到真正的flag，但我们已经知道了接下来的解题方向了，也不算是一无所获。

7.我们把key.log导出（追踪tcp流导出）

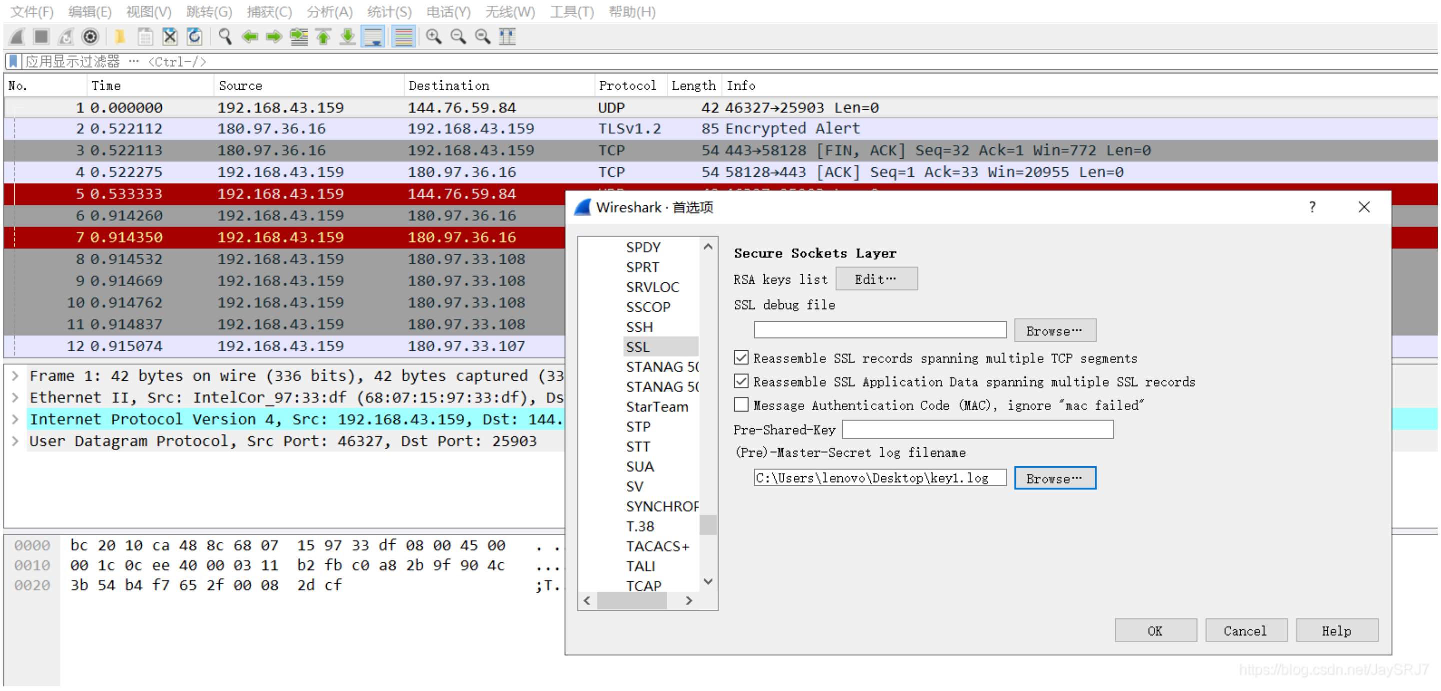

Wireshark · 追踪 TCP 流 (tcp.stream eq 58) · traffic

```
CLIENT_RANDOM cbdf25c6b2259a0b380b735427629e94abe5b070634c70bd9efd7ee76c0b9dc0
6782ad3aa5938c43831971a06e9a20eac27075d559799769ce5d1a3ea85211c981d8e67f75d6fd11fcf5536f331a968b
CLIENT_RANDOM 247f33720065429dc7e017e51f8b904309685ec8688296011cd3c53e5bafa75a
921ffbf7bfe6d8c393000f34eab6dc20486e620bdc90f21b6037c3df5592ef91fffca1dc8215699687a98febd45a4ce0
CLIENT_RANDOM 2000cef83c759e5e0c8bbdbd0a05388df25014fc32008610577ccd92d5fa3e3e
4c03f7a409b6e0ab7a0b793485696c02ab7743c1a9fda0039b0f7ac05205cf209d5855261ece18897dbe43a116b73627
CLIENT_RANDOM c5dd1755eff2a51b5d4a4990eca2cc201d9b637cd8ad217566f21194e19d6f60
c3a065698b99629875b03d6754597349612e6e7468ef66dcf8f277f9e84396ae55a1b72248019df1608ca3962f617252
CLIENT_RANDOM 11ae1440556a6e740fd9a18d0264cd4c49749355dcf7093daad965030a21fcfe
219786b326ccf760cd787de3cc7e1dcd668a1a3d336170334f879b061cec81131fff4850ce5c6ea15d907be8a36638b7
CLIENT_RANDOM 02002c43f43bc483152fa26cf255da81aa3048edf763c06e646c02dcd53f90fa
6a9b11b24d224c7c74691bfa8ac0086f8f027d8ec05e2135593425d42df5834aee37aedcfb9c2d476cb8998ce41603fb
CLIENT_RANDOM 444ba97e9d2ca12ec0c627db8ee5b5a97e1a4c49d3df77221e35c55ca3cc3c28
def07b2e4fc18939843a9409f742f243319705c862fac89a9002ed86d00e39401dedda9f9d7bfaa7e4c741ae3fb8500f
CLIENT_RANDOM ec6b0fc5b006e3ed50f2c682a2be2cad1fb04e92b29111f126725eefd1520b5b
cd3f903e551cb61140b7dd40ef3e8024bbdc3fc1c1e5737bbb2617b4a984b9c545e2468866080974a14791a19ac09671
CLIENT_RANDOM d4f49620d5e82b92f46041ef81fd7b12fc4423740ba5ee798e754b4f7a200b63
008815f111055f310026ac5e496e9f289ca6ed9c8cd9a3dc7c6fdd7dd54d25a0103c2ca48c4c0e4b54976cb572a8bba2
```



```
CLIENT_RANDOM f8d0b49ea5df02f0d61a5000eb0cbd529c8aea651e9ecd364c5deecfa3ecb4eb
b3d6d37d392432d4903b4fcb3bd7a52d2faf0552fe62e4a739bf19f611903cdd893cb8c34c2f895337c885491044b20f
CLIENT_RANDOM d219d102e23aec7e8bf0720968c5e18ffec8213ee91142ccff47460952c67557
33df1df41dcdf73f6d9a82ee9e75b8bb329bc52565b4861bf511853af59c670a972a5330627dc06cd8b7c24e3fad12ad
CLIENT_RANDOM c250e14706090035869fa0f2277538089fbedcb34c2ca4916c0cc14f7d03cd82
c7f36b2bf3902015802e44ea0139de8979a7886413782ff91b3e781d388b539c1e289f7ca9dad97e898d46a8f1d3a09b
CLIENT_RANDOM bf1e202c132e5ac68fde90dc21731b7ee8d37be63ccdf0379655eb33823fd316
a02c80340de4f380fd149ba49052b045ffa5a3cb43a6ee4958f3248f75459d7a548c38221550c1b456c23e37072d4297
CLIENT_RANDOM a61be0b892219f5110d62adf0379bc84cb3f8c670d027bdd02f7eeab0f4d6ab9
a155d79f8d678b2577a74c3de308090beeb501d5b7523d11067c6503fa93e0c275bd8b2916e262c8ac6221bf23fab2f5
CLIENT_RANDOM 41535597a84fbf6cc785687b0d043e59fc5e3786b5de125584b6134b52fdce64
589bdcc87a8da05d93101598073baf0da466297ebc143db4a8949a2a15ecf3e8e9691aeec1247590520c4e2217f9e93d
CLIENT_RANDOM 723c07e2d837f4c62e2a1009390631a147d36d06aa9c2d2341989a459b379738
c5975af83c0c9919ea3568de5ef4e005c97a7771102b598c3e25f9f0c4a84fff76553c7f2c545aaf3d1f393487845392
CLIENT_RANDOM 39eaf54df7641f4a6f409d07036f31b11ae94a6c6cbf0c69a6a5ee8f67253a2f
1da0035441cf07f31967d09edb879758c1a2940ae3a6faa53fcacf7061bf53be5fdf2dff7ddeabfcfa0a8099a2ced2e9
CLIENT_RANDOM dda8906b993d0a1e7f291a5b5231ac57dc6cb8f94b038c77d32e17a68ee07ccd
6ab7c0a696c8bf6e1f20d435fe36549af89872ea933de6a8b9964e9d5fc3ea66045fbb00802b0ffe8197a72ec529839b
CLIENT_RANDOM a6dd68eb537013b357631ab383c0a15902d3bb41fd5acd4f2149eb29b75a655b
8838ed7721f063615beab8e7033cce276e3be38585c35575bddd28d044f415d40fce77579e9e767649ba4411cc9cd2e4
CLIENT_RANDOM 840e5245e8f0cec707fc77958452ecbd974422c2cc3890b367972bc49a96d740
```

8.再导入密钥，编辑——>首选项——>ssl



```
No.   Time      Source          Destination     Protocol  Length Info
    1 0.000000  192.168.43.159  144.76.59.84    UDP       42 46327→25903 Len=0
    2 0.522112  180.97.36.16    192.168.43.159  TLSv1.2   85 Encrypted Alert
    3 0.522113  180.97.36.16    192.168.43.159  TCP       54 443→58128 [FIN, ACK] Seq=32 Ack=1 Win=772 Len=0
    4 0.522275  192.168.43.159  180.97.36.16    TCP       54 58128→443 [ACK] Seq=1 Ack=33 Win=20955 Len=0
    5 0.533333  192.168.43.159  144.76.59.84
    6 0.914260  192.168.43.159  180.97.36.16
    7 0.914350  192.168.43.159  180.97.36.16
    8 0.914532  192.168.43.159  180.97.33.108
    9 0.914669  192.168.43.159  180.97.33.108
   10 0.914762  192.168.43.159  180.97.33.108
   11 0.914837  192.168.43.159  180.97.33.108
   12 0.915074  192.168.43.159  180.97.33.107

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (33
> Ethernet II, Src: IntelCor_97:33:df (68:07:15:97:33:df), Ds
> Internet Protocol Version 4, Src: 192.168.43.159, Dst: 144.
> User Datagram Protocol, Src Port: 46327, Dst Port: 25903

0000  bc 20 10 ca 48 8c 68 07  15 97 33 df 08 00 45 00   . .
0010  00 1c 0c ee 40 00 03 11  b2 fb c0 a8 2b 9f 90 4c   ...
0020  3b 54 b4 f7 65 2f 00 08  2d cf                     ;T.
```

Secure Sockets Layer

RSA keys list Edit…

SSL debug file

Browse…

☑ Reassemble SSL records spanning multiple TCP segments

☑ Reassemble SSL Application Data spanning multiple SSL records

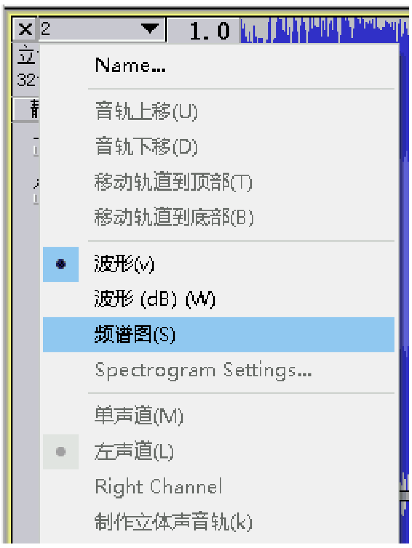
☐ Message Authentication Code (MAC), ignore "mac failed"

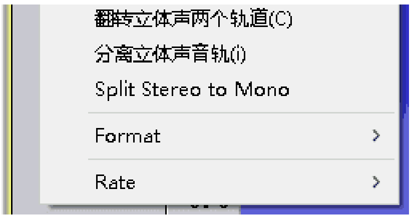
Pre-Shared-Key

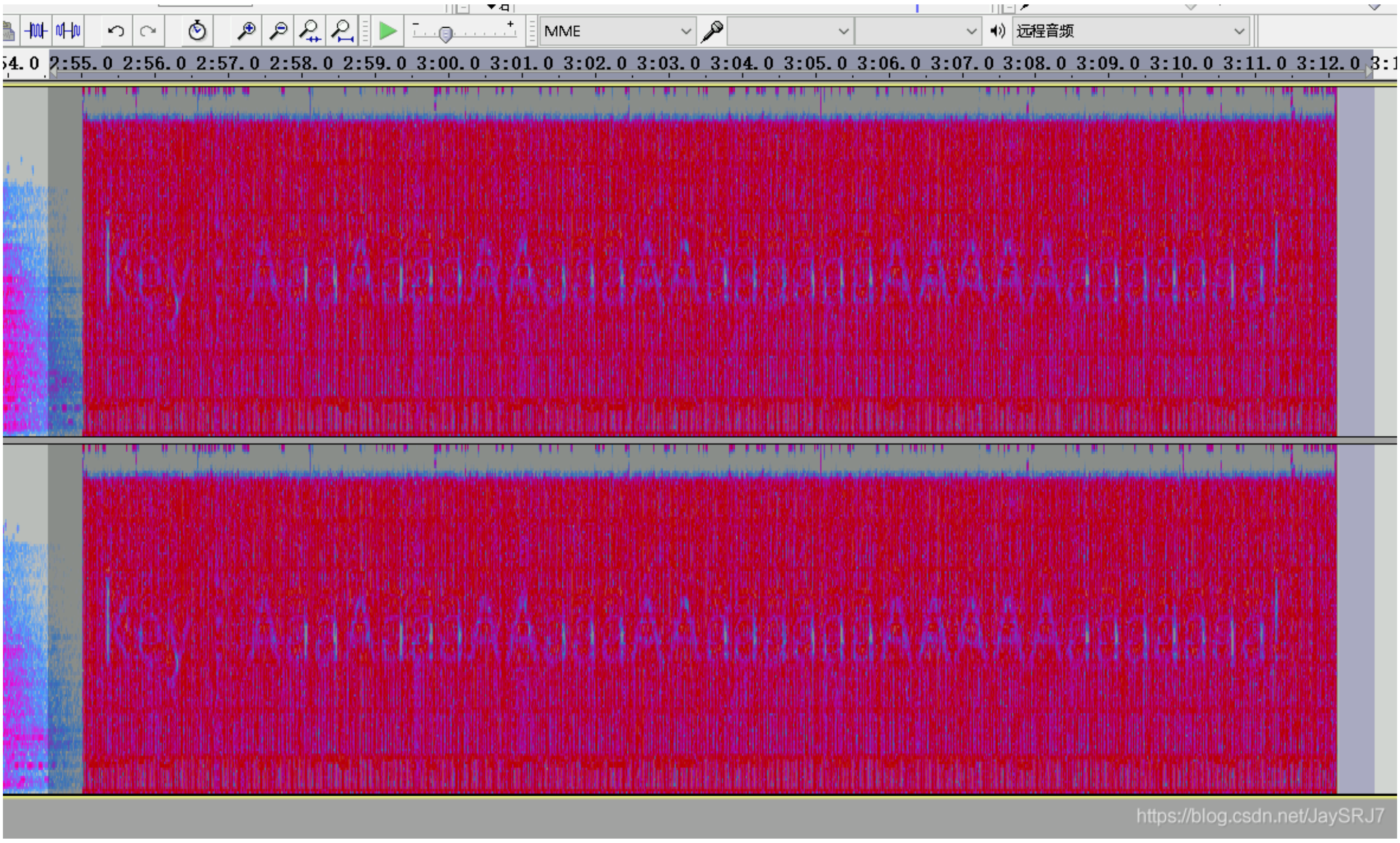
(Pre)-Master-Secret log filename

C:\Users\lenovo\Desktop\key1.log Browse…

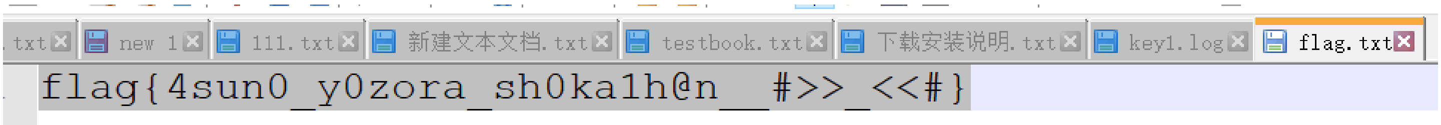
9.刷新之后出现解密后的流量包，在其中发现了一个隐藏的压缩包，解压出来是一个MP3音频，用Audacity打开，中间有一段杂音，用频谱图查看







10.发现是有隐藏密码的，提交发现不是flag，于是想到另一个压缩包，输入密码得到flag



```
flag{4sun0_y0zora_sh0ka1h@n__#>>_<<#}
```