

# 第三届上海市大学生网络安全大赛 流量分析 traffic WriteUp

原创

mutou990 于 2020-08-27 01:19:44 发布 540 收藏 1

分类专栏: CTF 文章标签: 安全

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/mutou990/article/details/108248461>

版权



CTF 专栏收录该内容

17 篇文章 1 订阅

订阅专栏

参考1: <https://www.cnblogs.com/sn1per/p/11835479.html>

参考2: <https://blog.csdn.net/JaySRJ7/article/details/102215248>

题目链接: <https://pan.baidu.com/s/1Ufq8W-NS4Af0xG-HqSbA> 提取码: 9wqs

解题思路:

打开流量包后, 按照协议进行分类, 发现了存在以下几种协议类型:

ARP / DNS / FTP / FTP-DATA / ICMP / ICMPv6 / IGMPv3 / LLMNR / NBNS / SSDP / SSL / TCP / TLSv1.2 / UDP

The screenshot displays a Wireshark interface for analyzing a traffic capture file named 'traffic.pcapng'. The main window shows a list of captured packets with columns for Time, Source, Destination, Protocol, Length, and Info. The packets are categorized into ARP and DNS. Below the packet list, the details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. At the bottom, the protocol statistics pane provides a breakdown of the traffic by protocol, showing that Ethernet and Internet Protocol Version 6 are the most prominent.

Protocol	按分组百分比	分组	按字节百分比	字节	比特/秒	End Packets	End Bytes	End Bits/s
Frame	100.0	17953	100.0	16633916	843 k	0	0	0
Ethernet	100.0	17953	1.5	251342	12 k	0	0	0
Internet Protocol Version 6	1.2	213	0.1	8520	432	0	0	0
User Datagram Protocol	1.0	178	0.0	1424	72	1	8	0
Link-local Multicast Name Resolution	0.0	2	0.0	44	2	2	44	2

Protocol	Count	Bytes	Count	Bytes	Count	Bytes	Count	Bytes
Domain Name System	1.0	175	0.1	21194	1074	175	21194	1074
Transmission Control Protocol	0.0	3	0.0	96	4	3	96	4
Internet Control Message Protocol v6	0.2	32	0.0	1012	51	32	1012	51
Internet Protocol Version 4	98.7	17726	2.1	354540	17 k	0	0	0
User Datagram Protocol	0.7	133	0.0	1064	53	116	928	47
Simple Service Discovery Protocol	0.1	12	0.0	2096	106	12	2096	106
NetBIOS Name Service	0.0	3	0.0	150	7	3	150	7
Link-local Multicast Name Resolution	0.0	2	0.0	44	2	2	44	2
Transmission Control Protocol	98.0	17585	96.1	15991818	811 k	15468	13840202	701 k
Secure Sockets Layer	11.9	2136	94.0	15642468	793 k	1920	15135530	767 k
Hypertext Transfer Protocol	0.4	64	41.5	6903889	350 k	32	43778	2220
Media Type	0.1	11	41.2	6849528	347 k	11	6850035	347 k
Line-based text data	0.0	3	0.0	73	3	3	73	3
JavaScript Object Notation	0.0	2	0.0	768	38	2	768	38
CompuServe GIF	0.1	16	0.0	680	34	16	680	34
Malformed Packet	0.0	4	0.0	0	0	4	0	0
FTP Data	0.2	28	0.2	29435	1492	28	29435	1492
File Transfer Protocol (FTP)	0.4	80	0.0	2069	104	80	2069	104
Data	0.1	21	0.0	2819	142	21	2819	142
Internet Group Management Protocol	0.0	5	0.0	80	4	5	80	4
Internet Control Message Protocol	0.0	3	0.0	52	2	3	52	2
Address Resolution Protocol	0.1	14	0.0	392	19	14	392	19

(这里可以在过滤输入框里输入FTP回车后，再对筛选过的包进行分析查看，也可以ctrl+F 查找【字符串】关键字ctrl+F 查找关键字flag或者flag的【十六进制】666c6167进行快速查找，下面直接用查找flag关键字方法)

应用显示过滤器: **flag** 查找 取消

No.	Time	Source	Destination	Protocol	Length	Info
0	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	UDP	42	46327 → 25903 Len=0
6	0.914260	192.168.43.159	180.97.36.16	TCP	54	58128 → 443 [FIN, ACK] Seq=1 Ack=33 Win=20955 Len=0
7	0.914350	192.168.43.159	180.97.36.16	TCP	54	58128 → 443 [RST, ACK] Seq=2 Ack=33 Win=0 Len=0
8	0.914532	192.168.43.159	180.97.33.108	TCP	54	58027 → 443 [FIN, ACK] Seq=1 Ack=1 Win=20950 Len=0
9	0.914669	192.168.43.159	180.97.33.108	TCP	54	58085 → 443 [FIN, ACK] Seq=1 Ack=1 Win=20954 Len=0
10	0.914762	192.168.43.159	180.97.33.108	TCP	54	58084 → 443 [FIN, ACK] Seq=1 Ack=1 Win=20954 Len=0
11	0.914837	192.168.43.159	180.97.33.108	TCP	54	58047 → 443 [FIN, ACK] Seq=1 Ack=1 Win=20955 Len=0
12	0.915074	192.168.43.159	180.97.33.107	TCP	1454	58066 → 443 [ACK] Seq=1 Ack=1 Win=20952 Len=1400 [TCP segment of a reassemb...
13	0.915090	192.168.43.159	180.97.33.107	TLSv1.2	816	Application Data
14	0.946456	180.97.36.16	192.168.43.159	TCP	54	443 → 58128 [ACK] Seq=33 Ack=2 Win=772 Len=0

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0  
 Ethernet II, Src: IntelCor\_97:33:4f (68:07:15:97:33:4f), Dst: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c)  
 Internet Protocol Version 4, Src: 192.168.43.159, Dst: 144.76.59.84  
 User Datagram Protocol, Src Port: 46327, Dst Port: 25903

分组详情 只是在INFO标题里搜关键词  
 分组字节流 是在详细内容里搜关键词  
 建议选择分组字节流

```

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

No.	Time	Source	Destination	Protocol	Length	Info
7402	17.381176	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6298395 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7403	17.381176	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6299795 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7404	17.381177	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6301195 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7405	17.381177	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6302595 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7406	17.381177	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6303995 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7407	17.381177	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6305395 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7408	17.381178	180.97.34.136	192.168.43.159	TLSv1.2	1249	[SSL segment of a reassembled PDU]

7409 17.381242 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6294419 Win=5364480 Len=0

7410 17.381399 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6297891 Win=5364480 Len=0

7411 17.381482 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6301363 Win=5364480 Len=0

7412 17.381527 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6304835 Win=5364480 Len=0

7413 17.381593 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6307990 Win=5364480 Len=0

7414 17.441227 182.254.217.142 192.168.43.159 FTP 106 Response: 227 Entering Passive Mode (182,254,217,142,47,56).

7415 17.441586 192.168.43.159 182.254.217.142 FTP 65 Request: RETR flag

Frame 7415: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface 0

Ethernet II, Src: IntelCor\_97:33:df (68:07:15:97:33:df), Dst: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c)

Internet Protocol Version 4, Src: 192.168.43.159, Dst: 182.254.217.142

Transmission Control Protocol, Src Port: 58106, Dst Port: 21, Seq: 7, Ack: 53, Len: 11

Source Port: 58106

Destination Port: 21

[Stream index: 34]

[TCP Segment Len: 11]

Sequence number: 7 (relative sequence number)

[Next sequence number: 18 (relative sequence number)]

Acknowledgment number: 53 (relative ack number)

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 20950

[Calculated window size: 20950]

[Window size scaling factor: -1 (unknown)]

Checksum: 0x16fe [unverified]

[Checksum Status: Unverified]

Hex dump:

```

0000 bc 20 10 ca 48 8c 68 07 15 97 33 df 08 00 45 00  . . .H.h. . .3...E.
0010 00 33 66 50 40 00 40 06 57 a0 c0 a8 2b 9f b6 fe  .3fP@.@. W...+...
0020 d9 8e e2 fa 00 15 e8 2e 84 6e 0d e2 c8 1c 50 18  .....n....p.
0030 51 d6 16 fe 00 00 52 45 54 52 20 66 6c 61 67 0d  Q.....RE TR flag.
0040 0a

```

Request arg (ftp.request.arg), 4 字节

分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.572 | 配置文件: Default

查找出来没有用，继续查找

应用显示过滤器: flag

No.	Time	Source	Destination	Protocol	Length	Info
7406	17.381177	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6303995 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7407	17.381177	180.97.34.136	192.168.43.159	TCP	1454	443 → 58146 [ACK] Seq=6305395 Ack=1871 Win=18176 Len=1400 [TCP segment of a...]
7408	17.381178	180.97.34.136	192.168.43.159	TLV	1249	[SSL segment of a reassembled PDU]
7409	17.381242	192.168.43.159	180.97.34.136	TCP	54	58146 → 443 [ACK] Seq=1871 Ack=6294419 Win=5364480 Len=0
7410	17.381399	192.168.43.159	180.97.34.136	TCP	54	58146 → 443 [ACK] Seq=1871 Ack=6297891 Win=5364480 Len=0
7411	17.381482	192.168.43.159	180.97.34.136	TCP	54	58146 → 443 [ACK] Seq=1871 Ack=6301363 Win=5364480 Len=0
7412	17.381527	192.168.43.159	180.97.34.136	TCP	54	58146 → 443 [ACK] Seq=1871 Ack=6304835 Win=5364480 Len=0
7413	17.381593	192.168.43.159	180.97.34.136	TCP	54	58146 → 443 [ACK] Seq=1871 Ack=6307990 Win=5364480 Len=0
7414	17.441227	182.254.217.142	192.168.43.159	FTP	106	Response: 227 Entering Passive Mode (182,254,217,142,47,56).
7415	17.441586	192.168.43.159	182.254.217.142	FTP	65	Request: RETR flag
7416	17.441941	192.168.43.159	182.254.217.142	TCP	66	58149 → 12088 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
7417	17.482047	182.254.217.142	192.168.43.159	TCP	66	12088 → 58149 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 W...
7418	17.482159	192.168.43.159	182.254.217.142	TCP	54	58149 → 12088 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
7419	17.522353	182.254.217.142	192.168.43.159	FTP	115	Response: 150 Opening BINARY mode data connection for flag (7 bytes).

[TCP Segment Len: 61]

Sequence number: 53 (relative sequence number)

[Next sequence number: 114 (relative sequence number)]

Acknowledgment number: 18 (relative ack number)

0101 .... = Header Length: 20 bytes (5)

Flags: 0x018 (PSH, ACK)

Window size value: 229

[Calculated window size: 229]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xc1c6 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

[SEQ/ACK analysis]

TCP payload (61 bytes)

File Transfer Protocol (FTP)

150 Opening BINARY mode data connection for flag (7 bytes).\r\n

Response code: File status okay; about to open data connection (150)

Response arg: Opening BINARY mode data connection for flag (7 bytes).

Hex dump:

```

0000 68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00  h...3.. .H...E.
0010 00 65 17 de 40 00 30 06 b5 e0 b6 fe d9 8e c0 a8  .e.@.0. ....
0020 2b 9f 00 15 e2 fa 0d e2 c8 1c e8 2e 84 79 50 18  +.....yP.
0030 00 e5 c1 c6 00 00 31 35 30 20 4f 70 65 6e 69 6e  .....15 0 Openin
0040 67 20 42 49 4e 41 52 59 20 6d 6f 64 65 20 64 61  g BINARY mode da
0050 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f  ta conne ction fo
0060 72 20 66 6c 61 67 20 28 37 20 62 79 74 65 73 29  r flag ( 7 bytes)
0070 2e 0d 0a

```

Response arg (ftp.response.arg), 55 字节

分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.572 | 配置文件: Default

open BINARY 也是没有用

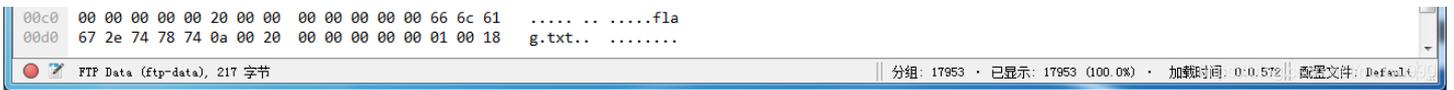
trafficpcapng

应用显示过滤器: flag

发现敏感信息 flag.zip  
应该联想到解题方向：解压后，里面有flag值  
RETR是下载 store是上传 PASV是FTP被动模式

继续查找后，发现压缩包内容，如下图

继续查找后，发现压缩包具体内容，应该联想到提取这个压缩包。  
注意FTP-DATA  
可以通过应用显示过滤器过滤想要查看的协议或方法  
如想查看ftp和ftp-data协议  
可以在过滤器栏输入ftp or ftp-data 回车



traffic.pcapng  
应用显示过滤器: <Ctrl-/> 表达式: + 应用此过滤器  
分组字节流 宽度 区分大小写 字符串 flag 查找 取消

No.	Time	Source	Destination	Protocol	Length	Info
8012	18.235276	192.168.43.159	144.76.59.84	UDP	42	46327 → 25903 Len=0
8013	18.824537	192.168.43.159	182.254.217.142	FTP	62	Request: TYPE I
8014	18.824638	192.168.43.159	144.76.59.84	UDP	42	46327 → 25903 Len=0
8015	18.882232	192.168.43.159	192.168.43.159	FTP	85	Response: 200 Switching to Binary mode.
8016	18.882494	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
8017	18.931501	182.254.217.142	192.168.43.159	FTP	108	Response: 227 Entering Passive Mode (182,254,217,142,120,115).
8018	18.931738	192.168.43.159	182.254.217.142	FTP	69	Request: RETR flag.zip
8019	18.932023	192.168.43.159	182.254.217.142	TCP	66	58150 → 30835 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
8020	18.963066	182.254.217.142	192.168.43.159	TCP	66	30835 → 58150 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
8021	18.963204	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
8022	19.002634	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes
8023	19.003254	182.254.217.142	192.168.43.159	TCP	54	30835 → 58150 [FIN, ACK] Seq=1 Ack=1 Win=29312 Len=0
8024	19.003254	182.254.217.142	192.168.43.159	FTP	121	Request: RETR flag.zip (217 bytes)
8025	19.003355	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [ACK] Seq=1 Ack=1 Win=5364608 Len=0

Frame 8022: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on interface  
Ethernet II, Src: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c), Dst: IntelCor\_97:33:df  
Internet Protocol Version 4, Src: 182.254.217.142, Dst: 192.168.43.159  
Transmission Control Protocol, Src Port: 30835, Dst Port: 58150, Seq: 1, Ack: 1, Window: 29312, Len: 217, Win=29312, Len=0, MSS=1400, WS=128, SACK\_PERM=1, Flags: 0x018 (PSH, ACK), Window size value: 229, [Calculated window size: 29312], [Window size scaling factor: 128], Checksum: 0x5442 [unverified], [Checksum Status: Unverified]

0050 08 00 00 00 66 6c 61 67 2e 74 78 74 a2 3c ed 3e ....flag .txt.<>  
0060 87 03 eb 29 41 f0 85 c5 4e cd 4d 63 1a 10 95 6d (...)A...N.Mc...m  
0070 42 79 61 d2 0a 38 9f b7 ab c0 8b 72 87 7f fc 3b Bya..8...r...;  
0080 18 c4 c5 5e ae a0 56 ab 71 1d 36 fa 34 56 cb 50 ...^..V. q.6.4V.P  
0090 4b 07 08 b6 03 57 d8 33 00 00 00 25 00 00 00 50 K...W.3 ...P  
00a0 4b 01 02 1f 00 14 00 09 00 08 00 7d b9 51 4b b6 K.....}.QK.  
00b0 03 57 d8 33 00 00 25 00 00 08 00 24 00 00 .W.3...% .....\$.  
00c0 00 00 00 00 20 00 00 00 00 00 00 66 6c 61 .....fla  
00d0 67 2e 74 78 74 0a 00 20 00 00 00 01 00 18 g.txt.. .....

tcp.stream eq 38 表达式: + 应用此过滤器  
分组字节流 宽度 区分大小写 字符串 flag 查找 取消

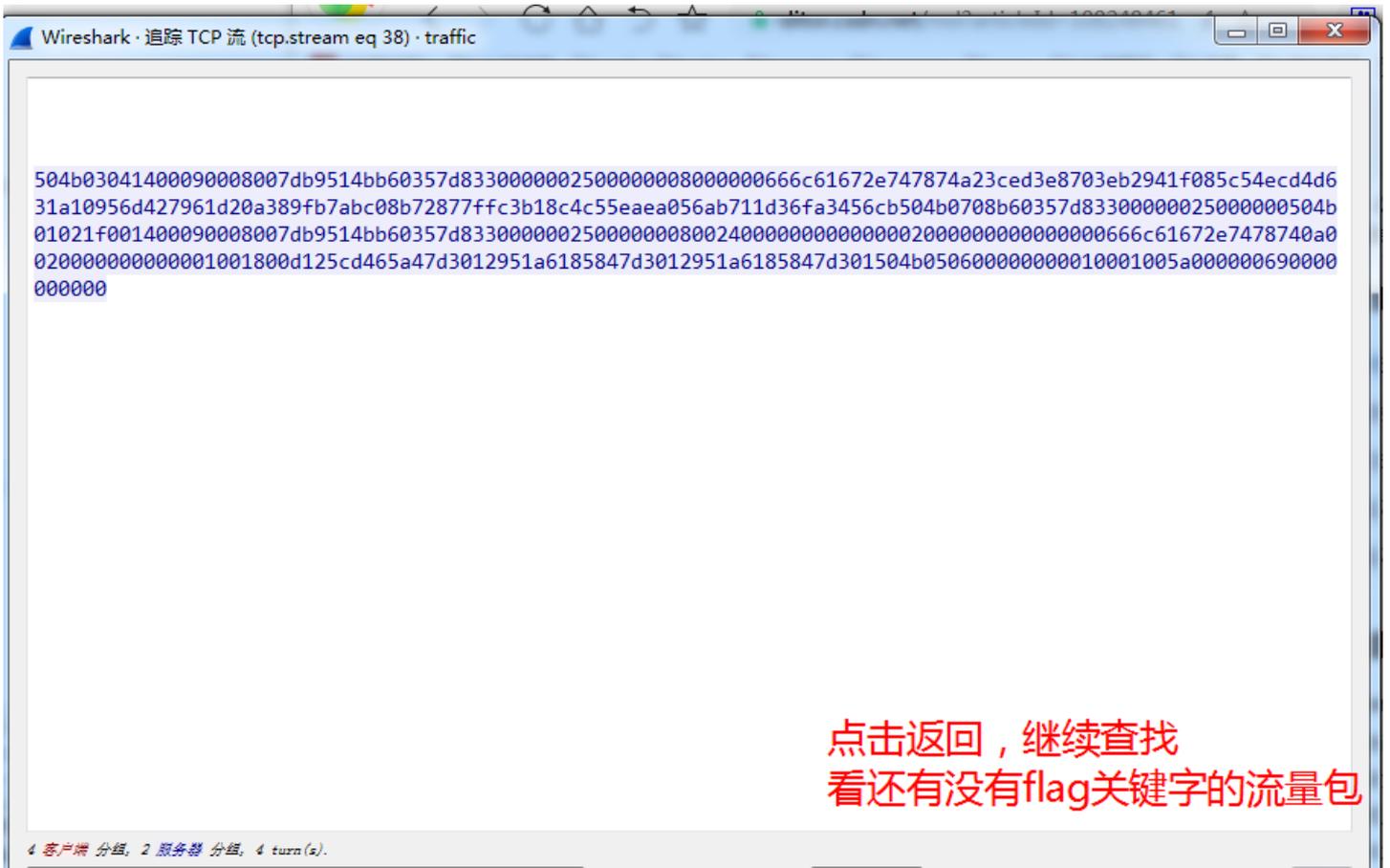
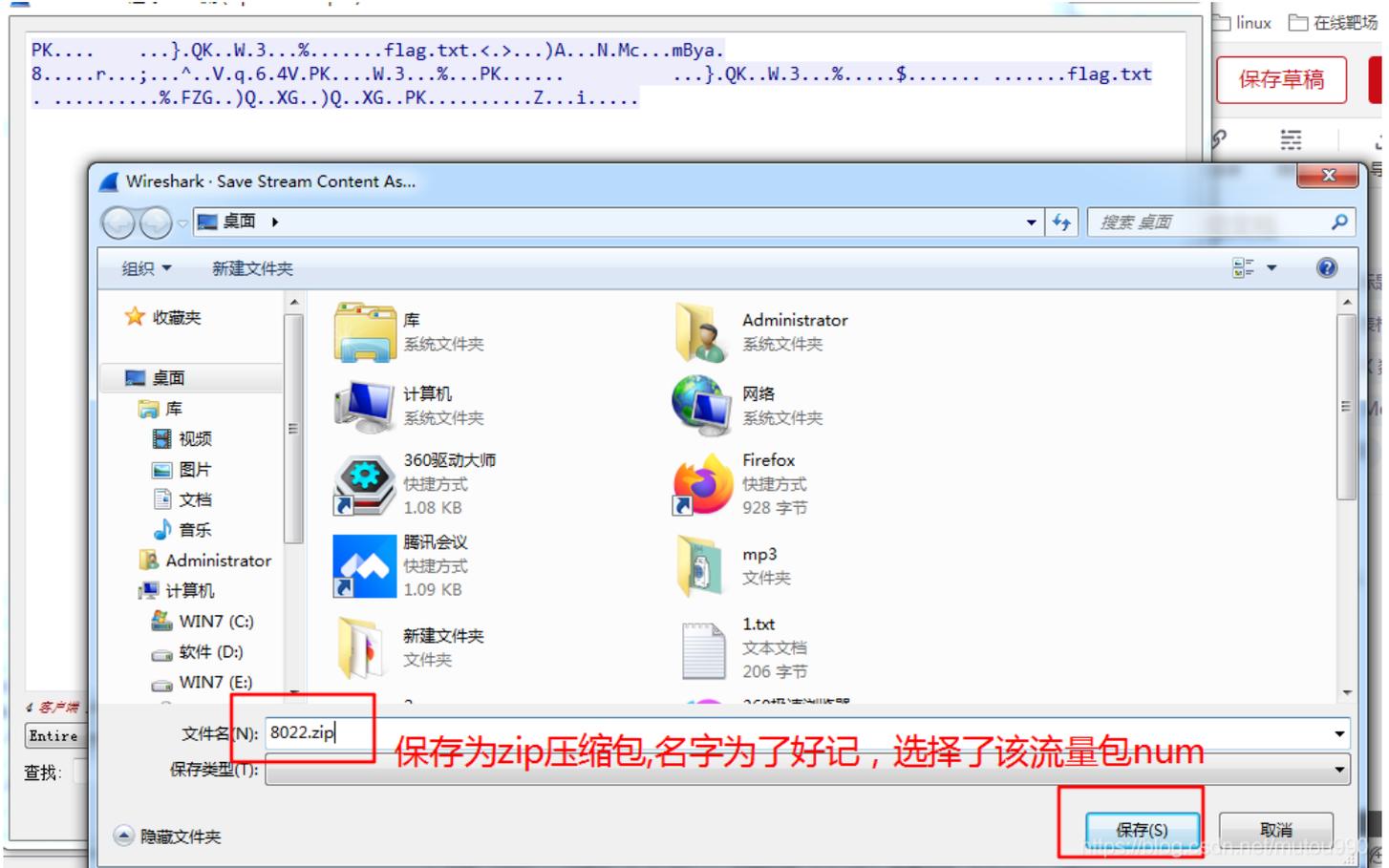
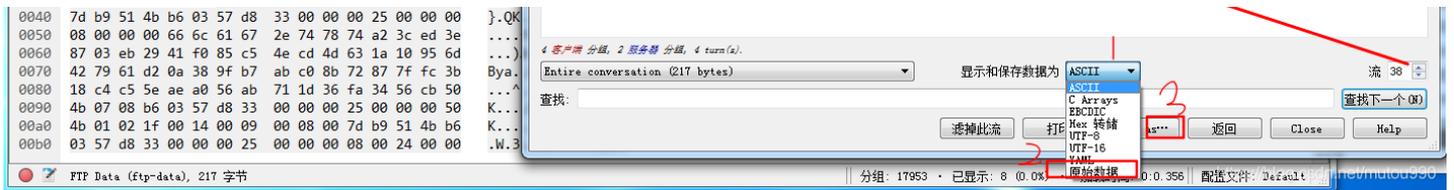
No.	Time	Source	Destination	Protocol	Length	Info
8019	18.932023	192.168.43.159	182.254.217.142	TCP	66	58150 → 30835 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
8020	18.963066	182.254.217.142	192.168.43.159	TCP	66	30835 → 58150 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=...
8021	18.963204	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
8022	19.002634	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes
8023	19.003254	182.254.217.142	192.168.43.159	TCP	54	30835 → 58150 [FIN, ACK] Seq=1 Ack=1 Win=29312 Len=0
8025	19.003355	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [ACK] Seq=1 Ack=219 Win=4194048 Len=0
8026	19.003778	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [FIN, ACK] Seq=1 Ack=219 Win=4194048 Len=0
8028	19.050593	182.254.217.142	192.168.43.159	TCP	54	30835 → 58150 [ACK] Seq=219 Ack=2 Win=29312 Len=0

Source Port: 30835  
Destination Port: 58150  
[Stream index: 38]  
[TCP Segment Len: 217]  
Sequence number: 1 (relative sequence number)  
[Next sequence number: 218 (relative sequence number)]  
Acknowledgment number: 1 (relative ack number)  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 229  
[Calculated window size: 29312]  
[Window size scaling factor: 128]  
Checksum: 0x5442 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
[SEQ/ACK analysis]  
TCP payload (217 bytes)  
FTP Data (217 bytes data)

0030 00 e5 54 42 00 00 50 4b 03 04 14 00 09 00 08 00 ..TB

Wireshark · 追踪 TCP 流 (tcp.stream eq 38) · traffic  
PK.... }.QK..W.3...%. ....flag.txt.<>...)A...N.Mc...mBya.  
8.....P...;...^..V.q.6.4V.PK...W.3...%.PK..... }.QK..W.3...%. ....\$. .....flag.txt  
.....%.FZG...).XG...).XG...PK.....Z..i.....

这是压缩包内容，可以看到里面有flag.txt



Entire conversation (217 bytes) 显示和保存数据为 原始数据 流 38

查找:  查找下一个(N)

滤掉此流 打印 Save as... 返回 Close Help

trafficpcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: Ctrl-1

No.	Time	Source	Destination	Protocol	Length	Info
8022	19.002634	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes
8023	19.003254	182.254.217.142	192.168.43.159	TCP	54	58106 → 21 [ACK] Seq=47 Ack=290 Win=20955 Len=0
8024	19.003254	182.254.217.142	192.168.43.159	FTP	121	Response: 150 Opening BINARY mode data connection for flag.zip (217 byt...
8025	19.003355	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [ACK] Seq=1 Ack=219 Win=4194048 Len=0
8026	19.003778	192.168.43.159	182.254.217.142	TCP	54	58150 → 30835 [FIN, ACK] Seq=1 Ack=219 Win=4194048 Len=0
8027	19.043439	192.168.43.159	182.254.217.142	TCP	54	58106 → 21 [ACK] Seq=47 Ack=290 Win=20955 Len=0
8028	19.050593	182.254.217.142	192.168.43.159	TCP	54	30835 → 58150 [ACK] Seq=219 Ack=2 Win=29312 Len=0
8029	19.051221	182.254.217.142	192.168.43.159	FTP	78	Response: 226 Transfer complete.
8030	19.092007	192.168.43.159	182.254.217.142	TCP	54	58106 → 21 [ACK] Seq=47 Ack=314 Win=20955 Len=0
8031	19.343730	192.168.43.159	144.76.59.84	UDP	42	46327 → 25903 Len=0
8032	19.828813	192.168.43.159	180.97.33.108	TCP	54	58047 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
8033	19.828860	192.168.43.159	144.76.59.84	UDP	42	46327 → 25903 Len=0
8034	19.830626	192.168.43.159	180.97.33.108	TCP	54	58027 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
8035	19.832577	192.168.43.159	180.97.33.108	TCP	54	58085 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0

[TCP Segment Len: 67]  
 Sequence number: 223 (relative sequence number)  
 [Next sequence number: 290 (relative sequence number)]  
 Acknowledgment number: 47 (relative ack number)  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 Window size value: 229  
 [Calculated window size: 229]  
 [Window size scaling factor: -1 (unknown)]  
 Checksum: 0xf6dd [unverified]  
 [Checksum Status: Unverified]  
 Urgent pointer: 0  
 [SEQ/ACK analysis]  
 TCP payload (67 bytes)  
 File Transfer Protocol (FTP)  
 150 Opening BINARY mode data connection for flag.zip (217 bytes).\r\n  
 Response code: File status okay; about to open data connection (150)  
 Response arg: Opening BINARY mode data connection for flag.zip (217 bytes).

```

0000 68 07 15 97 33 df bc 20 10 ca 48 8c 08 00 45 00 h...3.. ..H...E.
0010 00 b6 17 e2 40 00 30 06 b5 d6 b6 fe d9 8e c0 a8 .k..@.0. ....
0020 2b 9f 00 15 e2 fa 0d e2 c8 c6 e8 2e 84 96 50 18 +.....P.
0030 00 e5 f6 dd 00 00 31 35 30 20 4f 70 65 6e 69 6e .....15 0 Openin
0040 67 20 42 49 4e 41 52 59 20 6d 6f 64 65 20 64 61 g BINARY mode da
0050 74 61 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 66 6f ta conne ction fo
0060 72 20 66 6c 61 67 2e 7a 69 70 20 28 32 31 37 20 r flag.z ip (217
0070 62 79 74 65 73 29 2e 0d 0a bytes)...
  
```

Response arg (ftp.response.arg), 61 字节

分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.308 · 配置文件: Default

只是记录以二进制模式打开压缩包。这个没用，继续查找

trafficpcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: Ctrl-1

No.	Time	Source	Destination	Protocol	Length	Info
8097	38.323554	192.168.43.159	180.149.145.242	TCP	54	58143 → 443 [ACK] Seq=219
8098	38.725500	220.181.7.165	192.168.43.159	TLSv1.2	85	Alert (Level: Warning, D
8099	38.725922	220.181.7.165	192.168.43.159	TCP	54	443 → 58144 [FIN, ACK] S
8100	38.725987	192.168.43.159	220.181.7.165	TCP	54	58144 → 443 [ACK] Seq=18
8101	40.263861	192.168.43.159	182.254.217.142	FTP	62	Request: TYPE I
8102	40.396026	182.254.217.142	192.168.43.159	FTP	85	Response: 200 Switching
8103	40.396286	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
8104	40.436442	182.254.217.142	192.168.43.159	FTP	108	Response: 227 Entering P
8105	40.436728	192.168.43.159	182.254.217.142	FTP	60	Request: LIST
8106	40.437062	192.168.43.159	182.254.217.142	TCP	66	58151 → 30629 [SYN, ACK] Seq=
8107	40.569868	182.254.217.142	192.168.43.159	TCP	66	30629 → 58151 [SYN, ACK] Seq=
8108	40.569868	182.254.217.142	192.168.43.159	TCP	54	21 → 58148 [ACK] Seq=280
8109	40.569955	192.168.43.159	182.254.217.142	TCP	54	58151 → 30629 [ACK] Seq=
8110	40.604411	182.254.217.142	192.168.43.159	FTP-DATA	437	FTP Data: 383 bytes

Frame 8110: 437 bytes on wire (3496 bits), 437 bytes captured (3496 bits) on interface 0  
 Ethernet II, Src: bc:20:10:ca:48:8c, Dst: IntelCor\_97:33:df (68:07:15:97:33:df)  
 Internet Protocol Version 4, Src: 182.254.217.142, Dst: 192.168.43.159  
 Transmission Control Protocol, Src Port: 30629, Dst Port: 58151, Seq: 1, Ack: 1, Len: 383  
 Source Port: 30629  
 Destination Port: 58151  
 [Stream index: 42]  
 [TCP Segment Len: 383]  
 Sequence number: 1 (relative sequence number)  
 [Next sequence number: 384 (relative sequence number)]  
 Acknowledgment number: 1 (relative ack number)  
 0101 .... = Header Length: 20 bytes (5)  
 Flags: 0x018 (PSH, ACK)  
 Window size value: 229  
 [Calculated window size: 29312]  
 [Window size scaling factor: 128]  
 Checksum: 0xb2a8 [unverified]  
 [Checksum Status: Unverified]

Wireshark - 追踪 TCP 流 (tcp.stream eq 42) - traffic

源地址	源端口	目标地址	目标端口	时间戳	标志	窗口大小	序列号	长度	应用层数据
dnwrxwrx-x	2 500	500	4096	Sep 17 23:44	docker				
-p--p--p--	1 33	33	7	Aug 16 18:51	flag				
-pwx-xp-x	1 33	33	217	Oct 18 01:10	flag.zip				
dnwrx-----	2 107	115	4096	Oct 17 17:38	gay				
dnwrxwrxwrx	2 0	0	16384	Oct 27 2016	lost+found				
dnwrxwrxwrx	3 0	0	4096	Nov 29 2016	test				

应该是FTP目录结构

没啥用，继续查找

有敏感信息，追踪流看一下

0120 20 4f 63 74 20 31 37 20 31 37 3a 33 38 20 67 61 Oct 17 17:38 ga

FTP Data (ftp-data), 383 字节 | 分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.308 | 配置文件: Default | https://blog.csdn.net/mulou990

trafficpcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: flag

No.	Time	Source	Destination	Protocol	Length	Info
8136	43.183124	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
8137	43.224221	182.254.217.142	192.168.43.159	FTP	107	Response: 227 Entering Passive Mode (182,254,217,142,31,103).
8138	43.224505	192.168.43.159	182.254.217.142	FTP	69	Request: RETR flag.zip
8139	43.224834	192.168.43.159	182.254.217.142	TCP	66	58153 → 8039 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
8140	43.271926	182.254.217.142	192.168.43.159	TCP	66	8039 → 58153 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
8141	43.272009	192.168.43.159	182.254.217.142	TCP	54	58153 → 8039 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
8142	43.303281	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes
8143	43.303965	182.254.217.142	192.168.43.159	TCP	54	8039 → 58153 [FIN, ACK] Seq=218 Ack=1 Win=29312 Len=0
8144	43.303966	182.254.217.142	192.168.43.159	FTP	121	Response: 150 Opening BINARY mode data connection for flag.zip (217 byt...
8145	43.304060	192.168.43.159	182.254.217.142	TCP	54	58153 → 8039 [ACK] Seq=1 Ack=219 Win=4194048 Len=0
8146	43.304374	192.168.43.159	182.254.217.142	TCP	54	58153 → 8039 [FIN, ACK] Seq=1 Ack=219 Win=4194048 Len=0
8147	43.343806	182.254.217.142	192.168.43.159	TCP	54	8039 → 58153 [ACK] Seq=219 Ack=2 Win=29312 Len=0
8148	43.344706	182.254.217.142	192.168.43.159	FTP	78	Response: 226 Transfer complete.
8149	43.344750	192.168.43.159	182.254.217.142	TCP	54	58106 → 21 [ACK] Seq=101 Ack=658 Win=20954 Len=0
8150	44.760513	192.168.43.159	182.254.217.142	FTP	71	Request: CWD /mdata/leav

Frame 8138: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0

Ethernet II, Src: IntelCor\_97:33:df (68:07:15:97:33:df), Dst: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c)

Internet Protocol Version 4, Src: 192.168.43.159, Dst: 182.254.217.142

Transmission Control Protocol, Src Port: 58106, Dst Port: 21, Seq: 86, Ack: 567, Len: 15

Source Port: 58106  
Destination Port: 21  
[Stream index: 34]  
[TCP Segment Len: 15]  
Sequence number: 86 (relative sequence number)  
[Next sequence number: 101 (relative sequence number)]  
Acknowledgment number: 567 (relative ack number)  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 67  
[Calculated window size: 67]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x7ba4 [unverified]  
[Checksum Status: Unverified]

0000 bc 20 10 ca 48 8c 68 07 15 97 33 df 08 00 45 00 ...H.h. ...3...E.  
0010 00 37 66 72 40 00 40 06 57 7a c0 a8 2b 9f b6 fe .7fr@.@. Wz...+...  
0020 d9 8e e2 fa 00 15 e8 2e 84 bd 0d e2 ca 1e 50 18 .....P.  
0030 00 43 7b a4 00 00 52 45 54 52 20 66 6c 61 67 2e .C(...RE TR flag.  
0040 7a 69 70 0d 0a zip..

Request arg (ftp.request.arg), 8 字节 | 分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.277 | 配置文件: Default

又找到一个flag.zip  
既可以像上面那个flag.zip那样，继续查找flag.zip的具体内容，然后提取出来该压缩包。也可以直接在8138上追踪流，本质是一样的。

trafficpcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: flag

No.	Time	Source	Destination	Protocol	Length	Info
8134	43.138928	192.168.43.159	182.254.217.142	FTP	62	Request: TYPE I
8135	43.182862	182.254.217.142	192.168.43.159	FTP	85	Response: 200 Switching to Binary mode.
8136	43.183124	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
8137	43.224221	182.254.217.142	192.168.43.159	FTP	107	Response: 227 Entering Passive Mode (182,254,217,142,31,103).
8138	43.224505	192.168.43.159	182.254.217.142	FTP	69	Request: RETR flag.zip
8139	43.224834	192.168.43.159	182.254.217.142	TCP	66	58153 → 8039 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
8140	43.271926	182.254.217.142	192.168.43.159	TCP	66	8039 → 58153 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
8141	43.272009	192.168.43.159	182.254.217.142	TCP	54	58153 → 8039 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
8142	43.303281	182.254.217.142	192.168.43.159	FTP-DATA	271	FTP Data: 217 bytes
8143	43.303965	182.254.217.142	192.168.43.159	TCP	54	8039 → 58153 [FIN, ACK] Seq=218 Ack=1 Win=29312 Len=0
8144	43.303966	182.254.217.142	192.168.43.159	FTP	121	Response: 150 Opening BINARY mode data connection for flag.zip (217 byt...
8145	43.304060	192.168.43.159	182.254.217.142	TCP	54	58153 → 8039 [ACK] Seq=1 Ack=219 Win=4194048 Len=0
8146	43.304374	192.168.43.159	182.254.217.142	TCP	54	58153 → 8039 [FIN, ACK] Seq=1 Ack=219 Win=4194048 Len=0
8147	43.343806	182.254.217.142	192.168.43.159	TCP	54	8039 → 58153 [ACK] Seq=219 Ack=2 Win=29312 Len=0
8148	43.344706	182.254.217.142	192.168.43.159	FTP	78	Response: 226 Transfer complete.

Frame 8138: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface 0

Ethernet II, Src: IntelCor\_97:33:df (68:07:15:97:33:df), Dst: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c)

Internet Protocol Version 4, Src: 192.168.43.159, Dst: 182.254.217.142

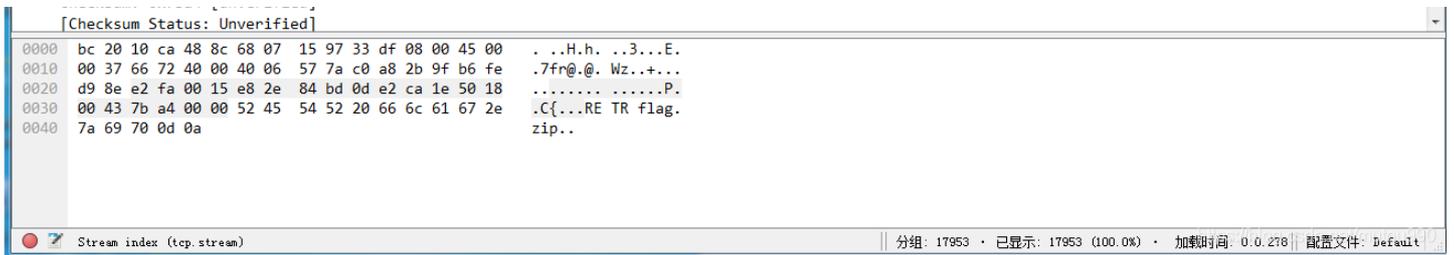
Transmission Control Protocol, Src Port: 58106, Dst Port: 21, Seq: 86, Ack: 567, Len: 15

Source Port: 58106  
Destination Port: 21  
[Stream index: 34]  
[TCP Segment Len: 15]  
Sequence number: 86 (relative sequence number)  
[Next sequence number: 101 (relative sequence number)]  
Acknowledgment number: 567 (relative ack number)  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window size value: 67  
[Calculated window size: 67]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x7ba4 [unverified]

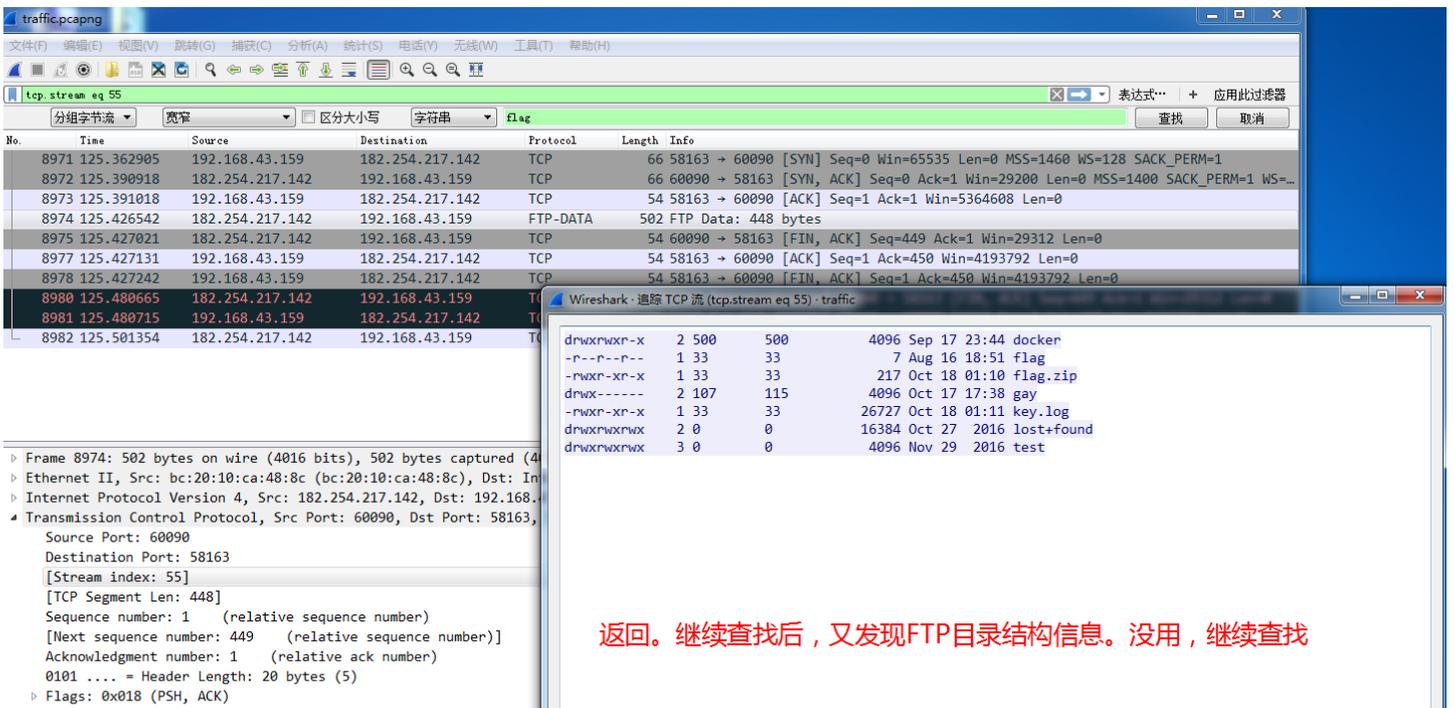
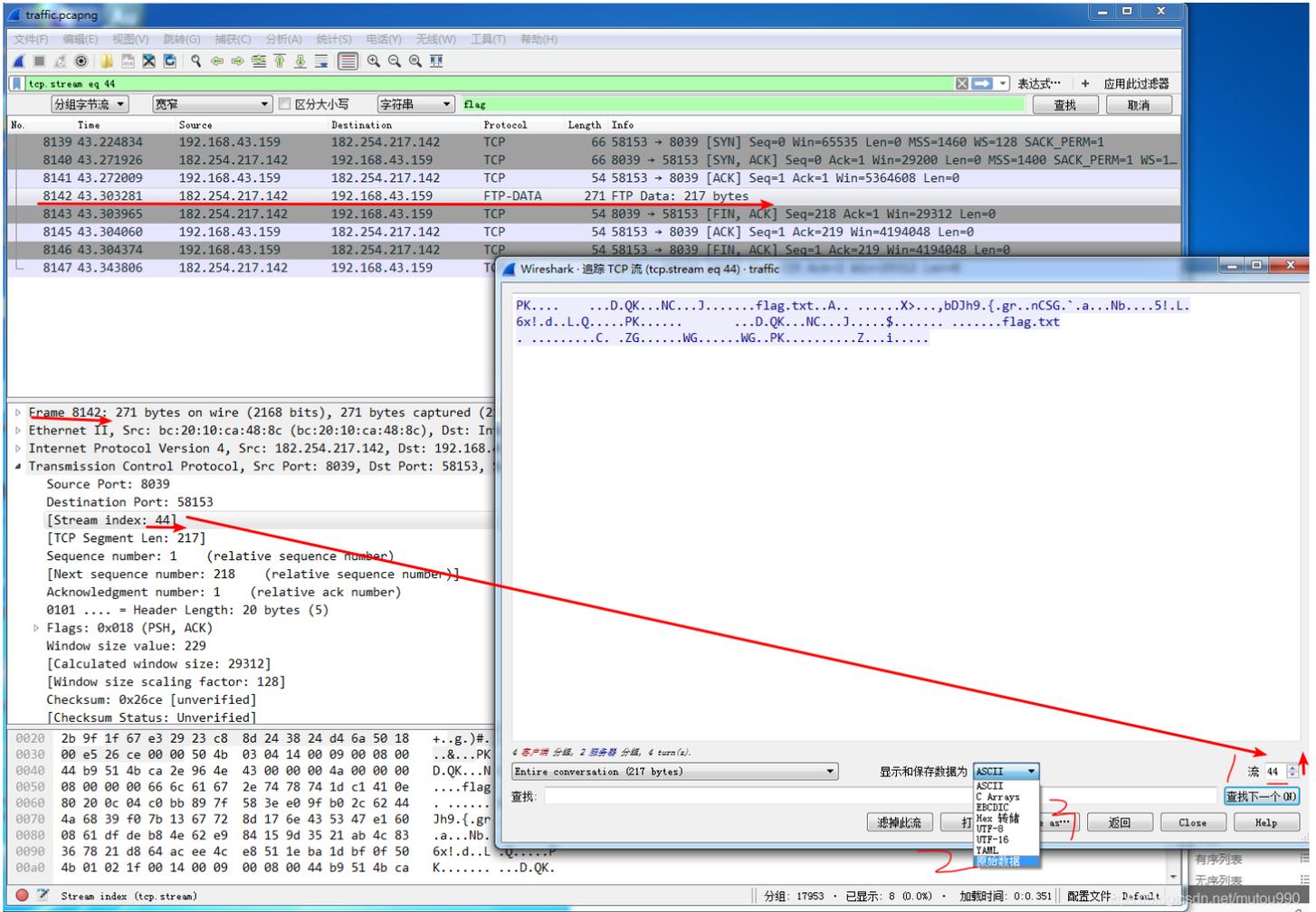
注意这里

标记/取消标记 分组(M) Ctrl+M  
忽略/取消忽略 分组(I) Ctrl+D  
设置/取消设置 时间参考 Ctrl+T  
时间平移... Ctrl+Shift+T  
分组注释... Ctrl+Alt+C  
编辑解析的名称  
作为过滤器应用  
准备过滤器  
对话过滤器  
对话着色  
SCTP  
追踪流  
复制  
协议首选项  
解码为(A)...  
在新窗口显示分组(W)

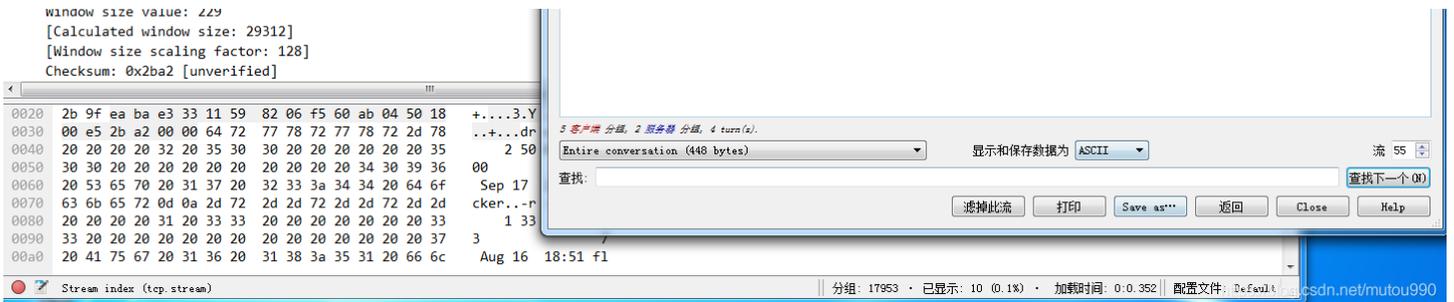
TCP 流  
UDP 流  
SSL 流  
HTTP 流



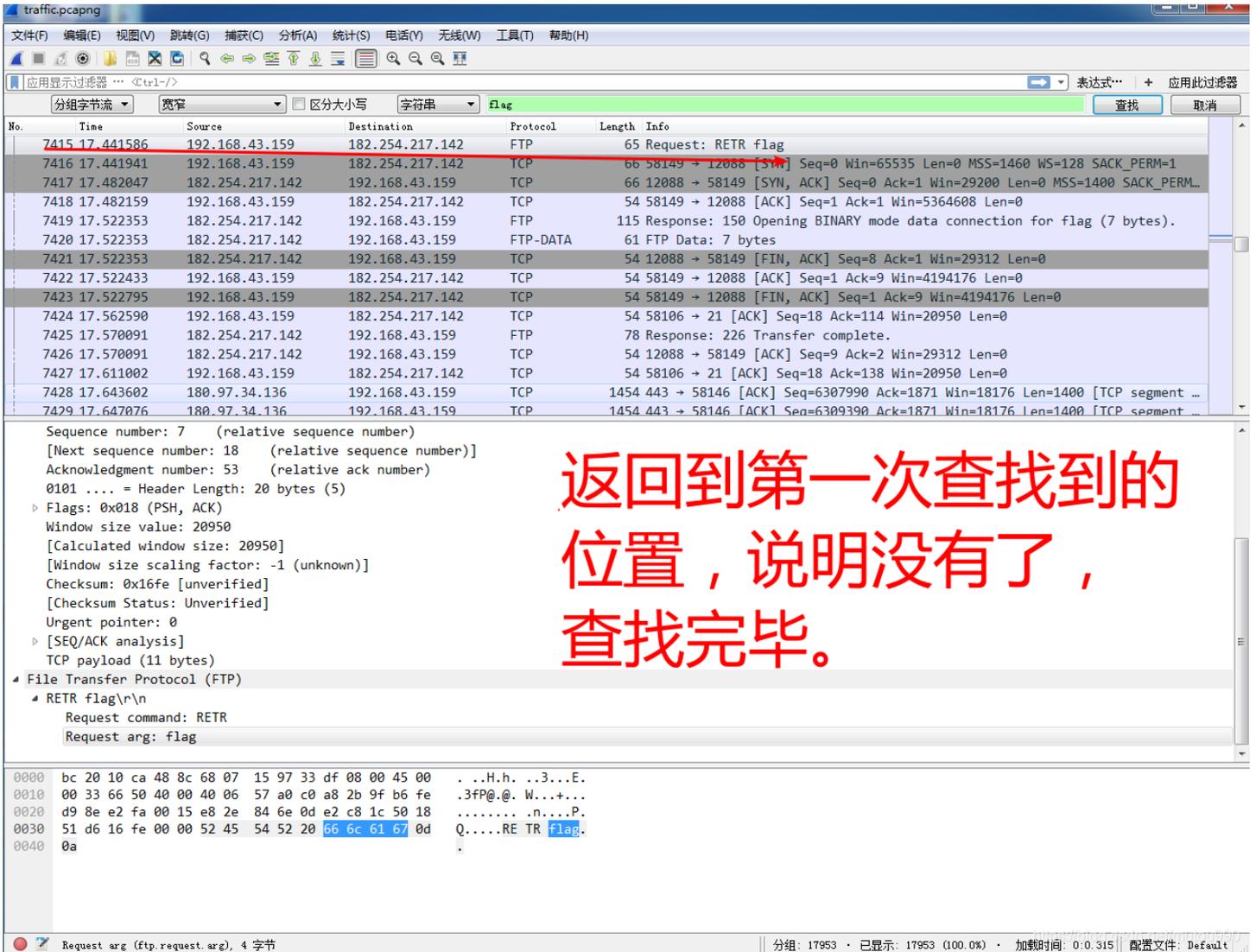
点击流的向上按钮



返回。继续查找后，又发现FTP目录结构信息。没用，继续查找



注意这里有一个key.log文件



返回到第一次查找到的位置，说明没有了，查找完毕。



# 两个压缩包，都需要解密密码

大小: 1 KB 共 1 个文件 压缩率 90.5%

<https://blog.csdn.net/mulou990>

而80221提示文件损坏，所以它才是需要解密的真压缩包。

用HxD分别打开8022.zip和8142.zip，分别修改09->00 然后另存为80221.zip和81421.zip.发现81421里面的flag.txt可以顺利打开，他是伪加密

<https://blog.csdn.net/mulou990>

提示有加密包，联想到之前发现的key.log

<https://blog.csdn.net/mulou990>

解密后从压缩包中提取到了一个flag.txt，打开发现是真的flag，并提示“maybe you should focus on the encrypted packets...”，意思是“也许你应该关注加密的数据包...”

下面提取key.log文件

traffic.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: <Ctrl-L/>

分组长节流 宽窄 区分大小写 字符串 key.log 查找 取消

No.	Time	Source	Destination	Protocol	Length	Info
9012	127.435251	192.168.43.159	182.254.217.142	FTP	67	Request: CWD /mydata
9013	127.482333	182.254.217.142	192.168.43.159	FTP	91	Response: 250 Directory successfully changed.
9014	127.529755	192.168.43.159	182.254.217.142	TCP	54	58165 → 21 [ACK] Seq=73 Ack=217 Win=17152 Len=0
9015	128.189549	192.168.43.159	182.254.217.142	FTP	62	Request: TYPE I
9016	128.241250	182.254.217.142	192.168.43.159	FTP	85	Response: 200 Switching to Binary mode.
9017	128.241526	192.168.43.159	182.254.217.142	FTP	60	Request: PASV
9018	128.291487	182.254.217.142	192.168.43.159	FTP	105	Response: 227 Entering Passive Mode (182,254,217,142,72,7).
9019	128.291976	192.168.43.159	182.254.217.142	FTP	68	Request: RETR key.log
9020	128.292317	192.168.43.159	182.254.217.142	TCP	66	58166 → 18439 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
9021	128.341598	182.254.217.142	192.168.43.159	TCP	66	18439 → 58166 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1
9022	128.341690	192.168.43.159	182.254.217.142	TCP	54	58166 → 18439 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
9023	128.390382	182.254.217.142	192.168.43.159	TCP	54	21 → 58165 [ACK] Seq=299 Ack=101 Win=29312 Len=0
9024	128.392743	182.254.217.142	192.168.43.159	FTP-DATA	1454	FTP Data: 1400 bytes
9025	128.392744	182.254.217.142	192.168.43.159	FTP-DATA	1454	FTP Data: 1400 bytes
9026	128.392829	192.168.43.159	182.254.217.142	TCP	54	58166 → 18439 [ACK] Seq=1 Ack=2801 Win=5364608 Len=0

Frame 9019: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0

Interface id: 0 (\Device\NPF\_{4BFDDBC3-E964-4672-B0EB-016775AFA79F})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 18, 2017 01:11:59.901660000 中国标准时间

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1508260319.901660000 seconds

```

0000 bc 20 10 ca 48 8c 68 07 15 97 33 df 08 00 45 00 ...H.h...E.
0010 00 36 66 98 40 00 40 06 57 55 c0 a8 2b 9f b6 fe .6f.@.WU.+..
0020 d9 8e e3 35 00 15 c7 13 e2 14 8b 95 78 8b 50 18 ...5....x.P.
0030 00 43 ca b8 00 00 52 45 54 52 20 6b 65 79 2e 6c .C...RE TR key.1
0040 6f 67 0d 0a ..og..

```

<https://blog.csdn.net/mutou990>

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

```

CLIENT_RANDOM cbd725c6b2259a0b380b735427629e94abe5b070634c70bd9efd7ee76c0b9dc0
6782ad3aa5938c43831971a06e9a20eac27075d559799769ce5d1a3ea85211c981d8e67f75d6fd11fcf5536f331a968b
CLIENT_RANDOM 247f33720065429dc7e017e51f8b904309685ec8688296011cd3c53e5bafa75a
921ffb7f7be6d8c393000f34eab6dc20486e620bdc90f21b6037c3df5592ef91fffca1dc8215699687a98febd45a4ce0
CLIENT_RANDOM 2000cef83c759e5e0c8bbdbd0a05388df25014fc32008610577ccd92d5fa3e3e
4c03f7a409b6e0ab7a0b793485696c02ab7743c1a9fdad0039b0f7ac05205cf209d5855261ece18897dbe43a116b73627
CLIENT_RANDOM c5dd1755eff2a51b5d4a4990eca2cc201d9b637cd8ad217566f21194e19d6f60
c3a065698b99629875b03d6754597349612e6e7468ef66dcf8f277f9e84396ae55a1b72248019df1608ca3962f617252
CLIENT_RANDOM 11ae1440556a6e740fd9a18d0264cd4c49749355dcf7093daad965030a21fcfe
219786b326ccf760cd787de3cc7e1dcd668a1a3d336170334f879b061cec81131fff4850ce5c6ea15d907be8a36638b7
CLIENT_RANDOM 02002c43f43bc483152fa26cf255da81aa3048edf763c06e646c02dcd53f90fa
6a9b11b24d224c7c74691bfa8ac0086f8f027d8ec05e2135593425d42df5834aee37aedcfb9c2d476cb8998ce41603fb
CLIENT_RANDOM 444ba97e9d2ca12ec0c627db8ee5b5a97e1a4c49d3df77221e35c55ca3cc3c28
def07b2e4fc18939843a9409f742f243319705c862fac89a9002ed86d00e39401dedda9f9d7bfaa7e4c741ae3fb8500f
CLIENT_RANDOM ec6b0fc5b006e3ed50f2c682a2be2cad1fb04e92b29111f126725eef1520b5b
cd3f903e551cb61140b7dd40ef3e8024bbdc3fc1c1e5737bbb2617b4a984b9c545e2468866080974a14791a19ac09671
CLIENT_RANDOM d4f49620d5e82b92f46041ef81fd7b12fc4423740ba5ee798e754b4f7a200b63
008815f111055f310026ac5e496e9f289ca6ed9c8cd9a3dc7c6fdd7dd54d25a0103c2ca48c4c0e4b54976cb572a8bba2
CLIENT_RANDOM f8d0b49ea5df02f0d61a5000eb0cbd529c8aea651e9ecd364c5deecfa3ecb4eb
b3d6d37d392432d4903b4fcb3bd7a52dfaf0552fe62e4a739bf19f611903cdd893cb8c34c2f895337c885491044b20f
CLIENT_RANDOM d219d102e23aec7e8bf0720968c5e18ffec8213ee91142ccff47460952c67557
33df1df41dcdcf73f6d9a82ee9e75b8bb329bc52565b4861bf511853af59c670a972a5330627dc06cd8b7c24e3fad12ad
CLIENT_RANDOM c250e14706090035869fa0f2277538089fbecb34c2ca4916c0cc14f7d03cd82
c7f36b2bf3902015802e44ea0139de8979a7886413782ff91b3e781d388b539c1e289f7ca9dad97e898d46a8f1d3a09b
CLIENT_RANDOM bf1e20c132e5ac68fde90dc21731b7ee8d37be63ccd0f0379655eb33823fd316
a02c80340de4f380f419ba49052b045ffa5a3cb43aeae4958f3248f75459d7a548c38221550c1b456c23e37072d4297
CLIENT_RANDOM a61be0b892219f5110d62ad0f379bc84cb3f8c670d027bdd02f7eeab0f4d6ab9
a155d79f8d678b2577a74c3de308090beeb501d5b7523d11067c6503fa93e0c275bd8b2916e262c8ac6221bf23fab2f5
CLIENT_RANDOM 41535597a84fbf6cc785687b0d043e59fc5e3786b5de125584b6134b52fdce64
589bdcc87a8da05d93101598073baf0da466297ebc143db4a8949a2a15ecf3e8e9691aeecc1247590520c4e2217f9e93d
CLIENT_RANDOM 723c07e2d837f4c62e2a1009390631a147d36d06aa9c2d2341989a459b379738

```

13 客户端 分组, 21 服务器 分组, 12 turn(s).

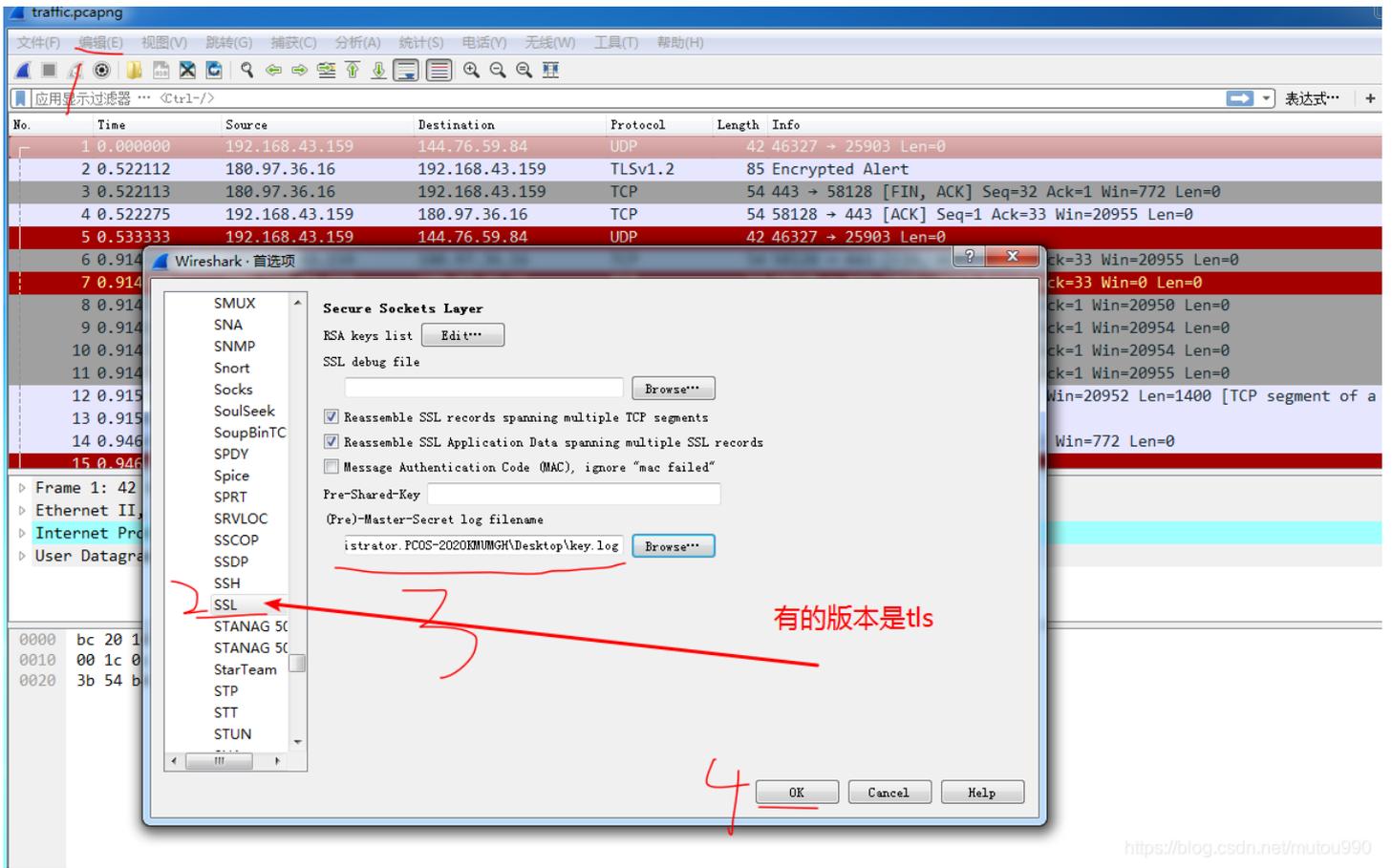
Entire conversation (26 kB) 显示和保存数据为 ASCII 流

查找: 查找下一个(N)

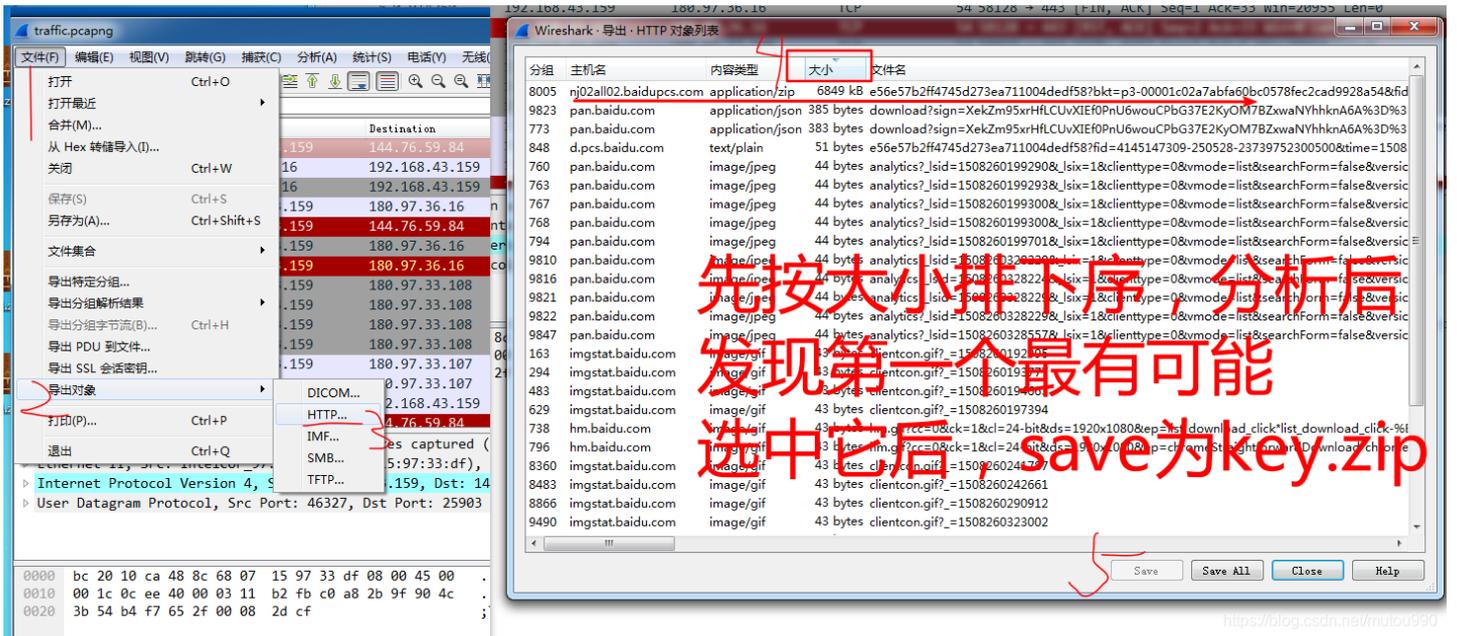
滤掉此流 打印 Save as... 返回 Close Help

<https://blog.csdn.net/mutou990>

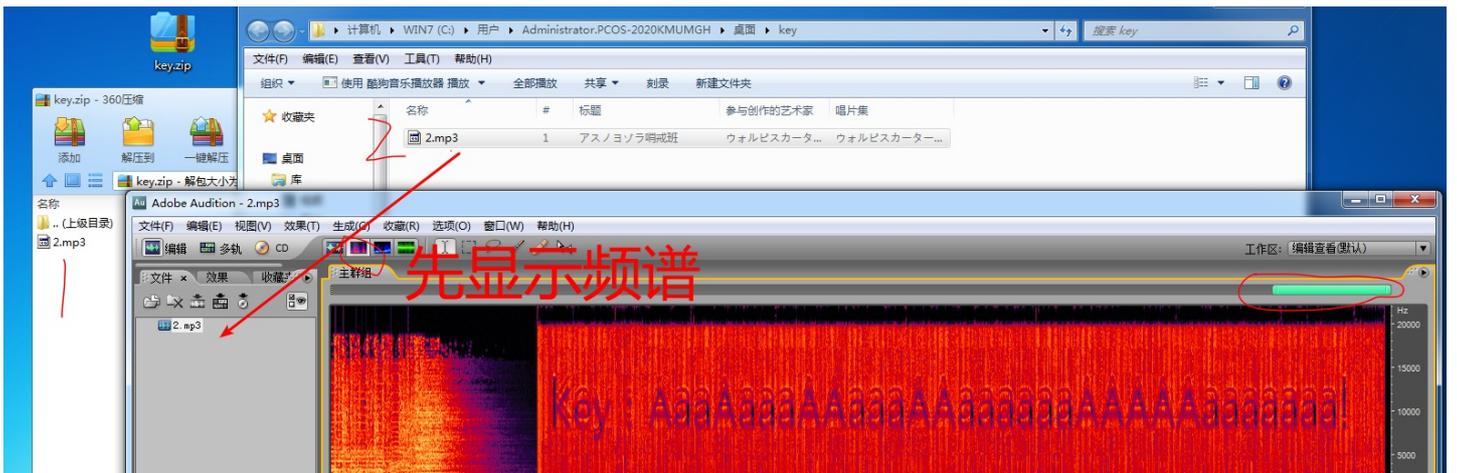
加密的数据包？那就应该是TLS协议没跑了，又想到key.log这个文件还没有用，然后使用key.log对TLS协议进行解密。（操作步骤：编辑→首选项→Protocols→TLS，然后在下面导入key.log文件）



<https://blog.csdn.net/mutou990>

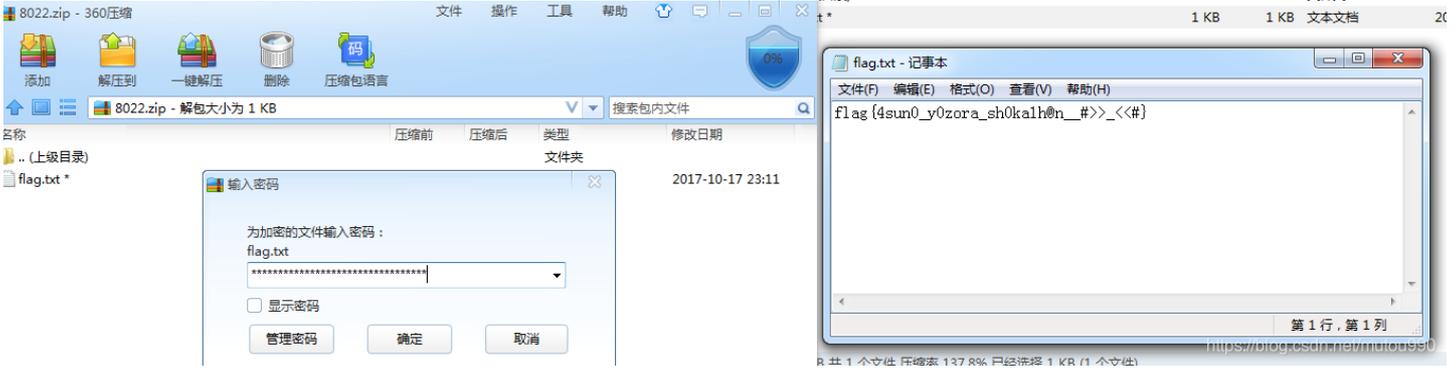


<https://blog.csdn.net/mutou990>





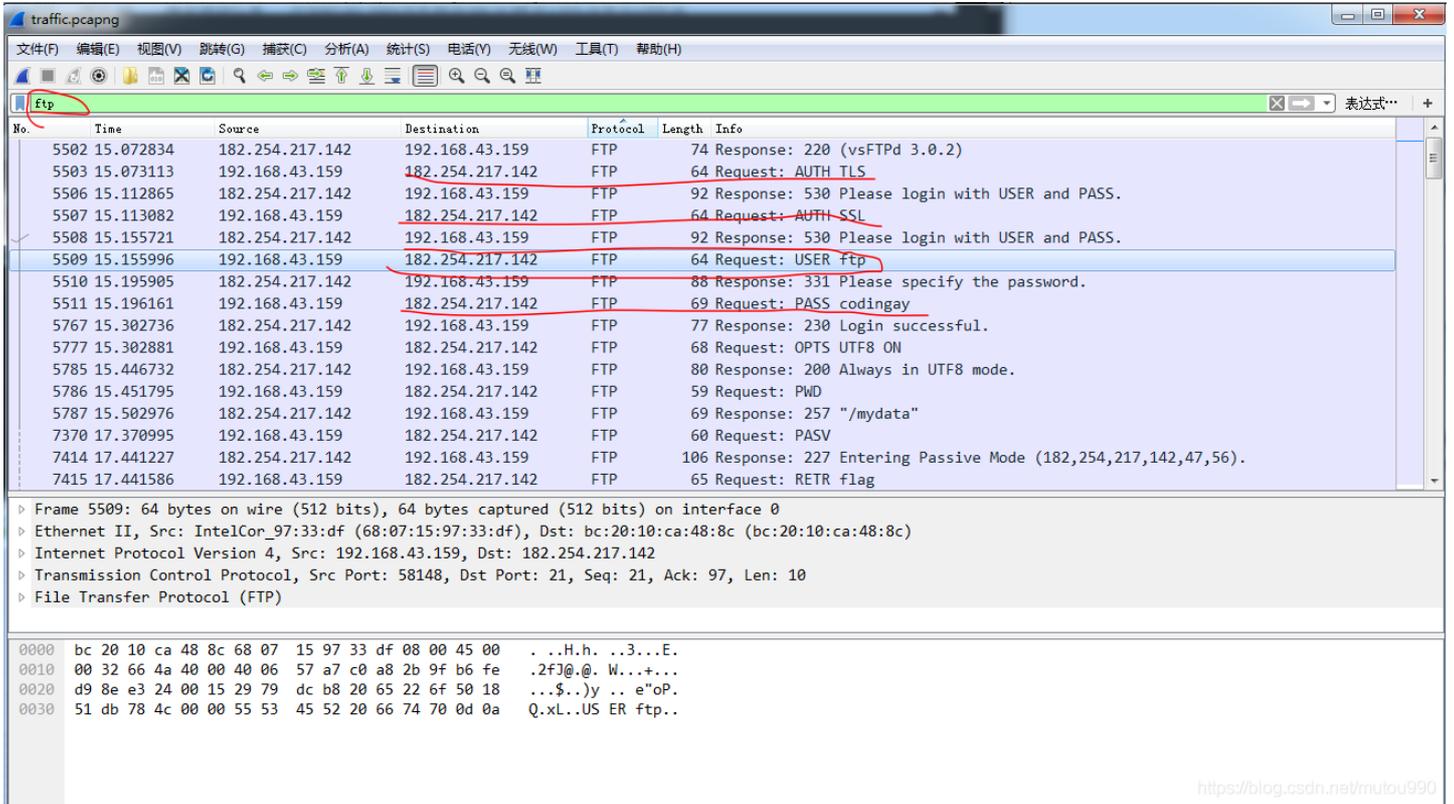
直接把该key提交flag,先试试，发现不对。那就解密压缩包



成功!

下面是别人有用的一部分思路，可以看看。

按照协议类型对数据包进行读取，发现只有FTP协议是用的，但是同时注意到TLS协议是进行加密的，其他的协议并没有什么作用。然后使用wireshark的过滤器将FTP和FTP-DATA筛选出来。发现了ftp的用户名和密码，尝试登陆，发现不能登录。



服务器地址: 182.254.217.142

用户名: ftp

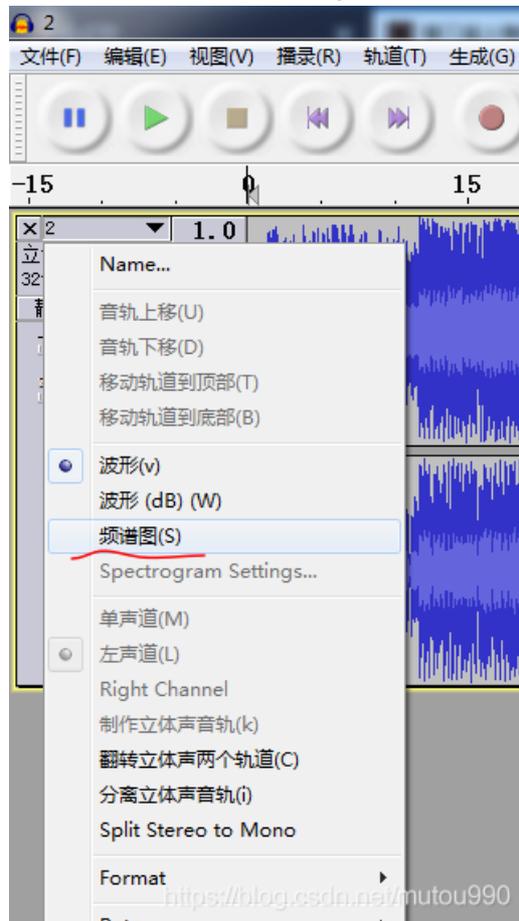
密码: codingay



(这里可以在过滤输入框里输入FTP回车后，再对筛选过的包进行分析查看，也可以ctrl+F 查找【字符串】关键字ctrl+F 查找关键字flag或者flag的【十六进制】666c6167进行快速查找，本文用查找flag关键字方法)

然后回到数据包刷新一下就可以看到揭秘之后的数据了。因为TLS加密的是http协议，所以解密之后直接过滤http协议就可以了。查看后可以大致分析出，是用百度网盘下了一个文件，把这个文件导出。(文件→导出对象→HTTP) 导出的文件是一个压缩包，解压后是一个音频文件，使用Audition打开，查看一下频谱帧率，可以看到用的是audacity不好用，看不清楚。

使用这个key可以解开刚才那个加了密的压缩文件，解压后拿到一个flag.txt，打开即可获得真正的flag!



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不不知道要得到真正的flag需要对这个流量包进行解密

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)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

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