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

本文链接：https://blog.csdn.net/mutou990/article/details/108248461

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

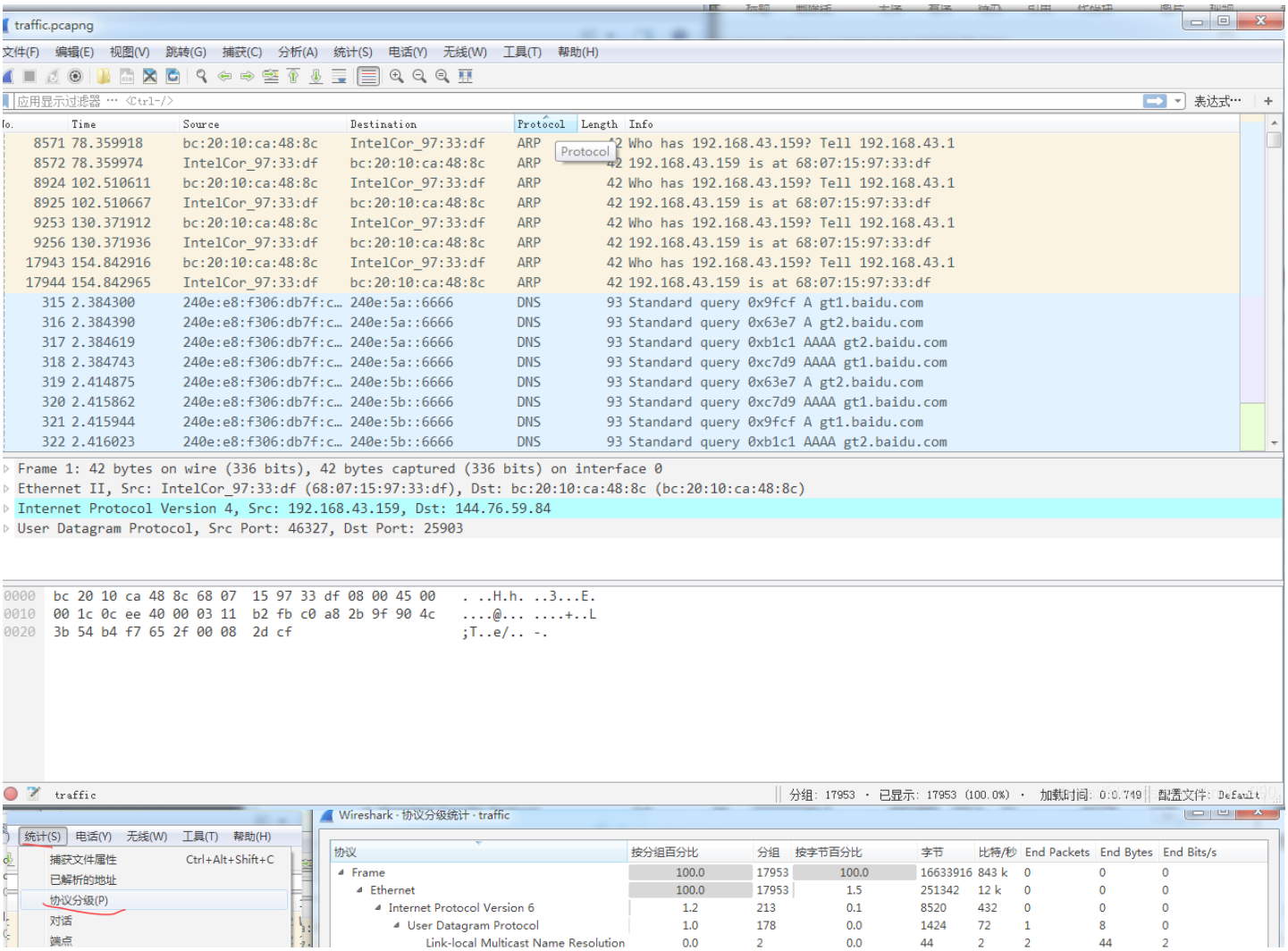
参考2：https://blog.csdn.net/JaySRJ7/article/details/102215248

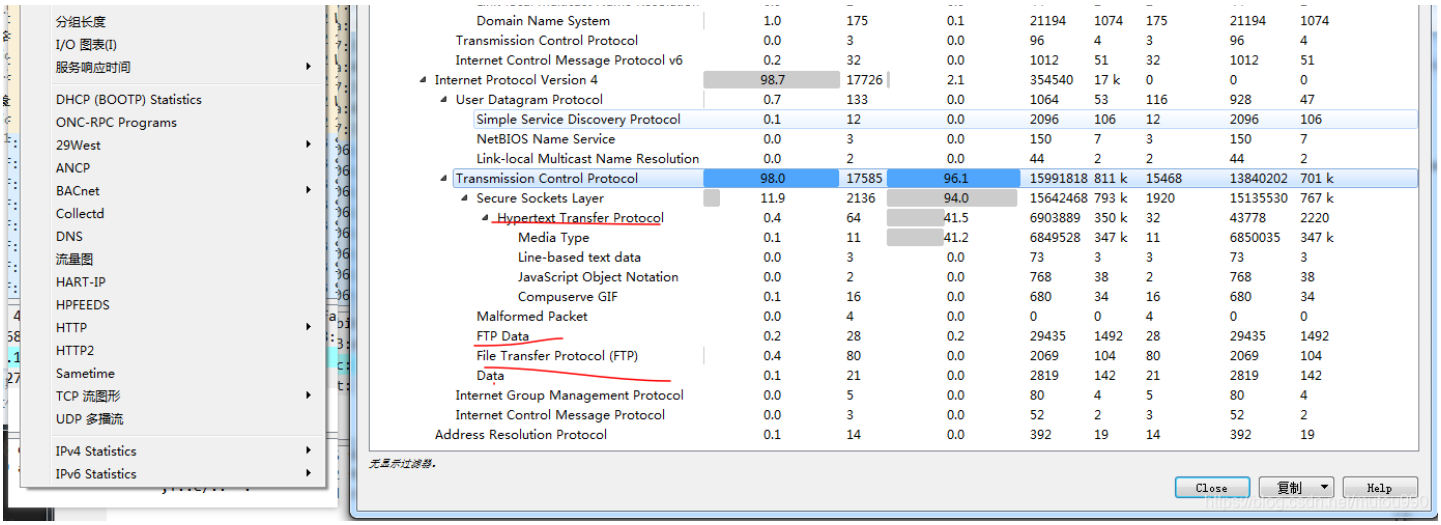
题目链接： https://pan.baidu.com/s/1Utfq8W-NS4Afl0xG-HqSbA 提取码: 9wqs

解题思路：

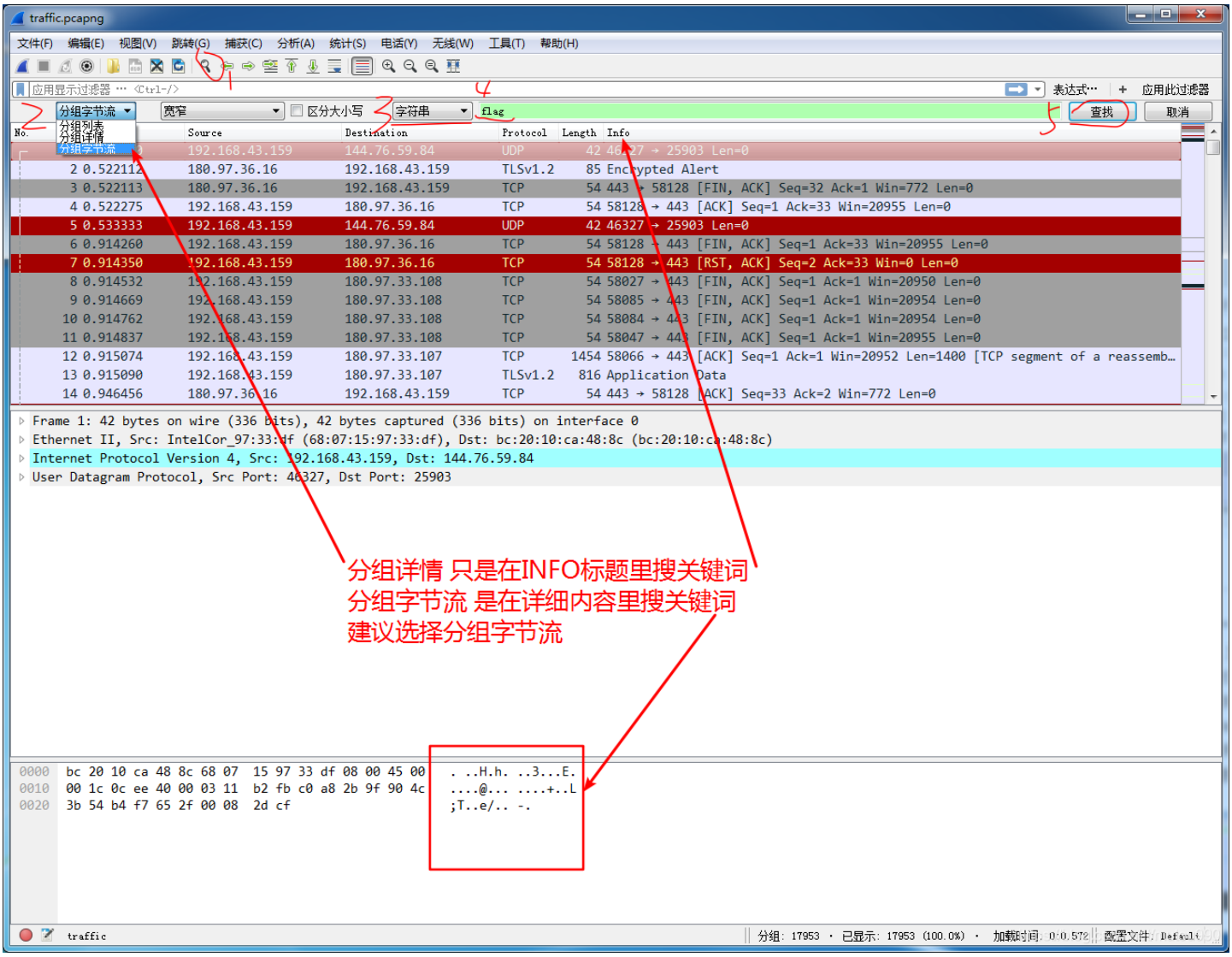
打开流量包后，按照协议进行分类，发现了存在以下几种协议类型：

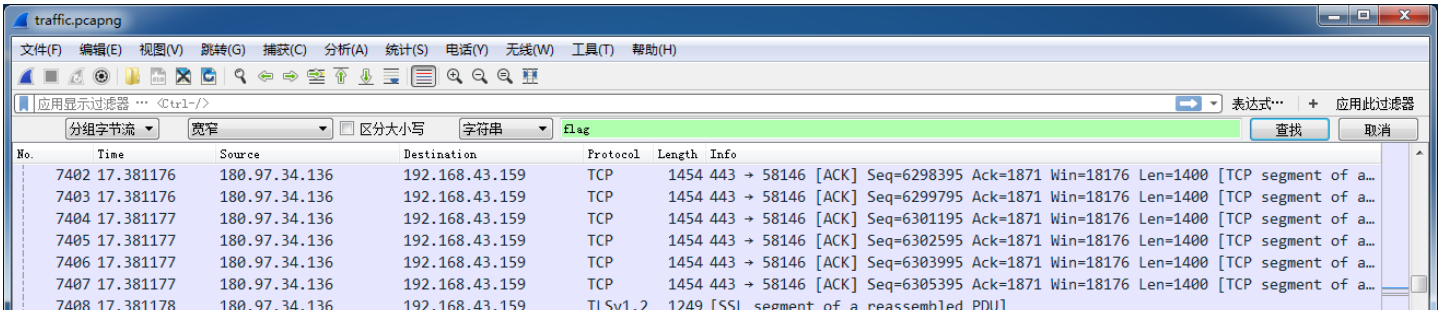
> ARP / DNS / FTP / FTP-DATA / ICMP / ICMPv6 / IGMPv3 / LLMNR / NBNS / SSDP / SSL / TCP / TLSv1.2 / UDP

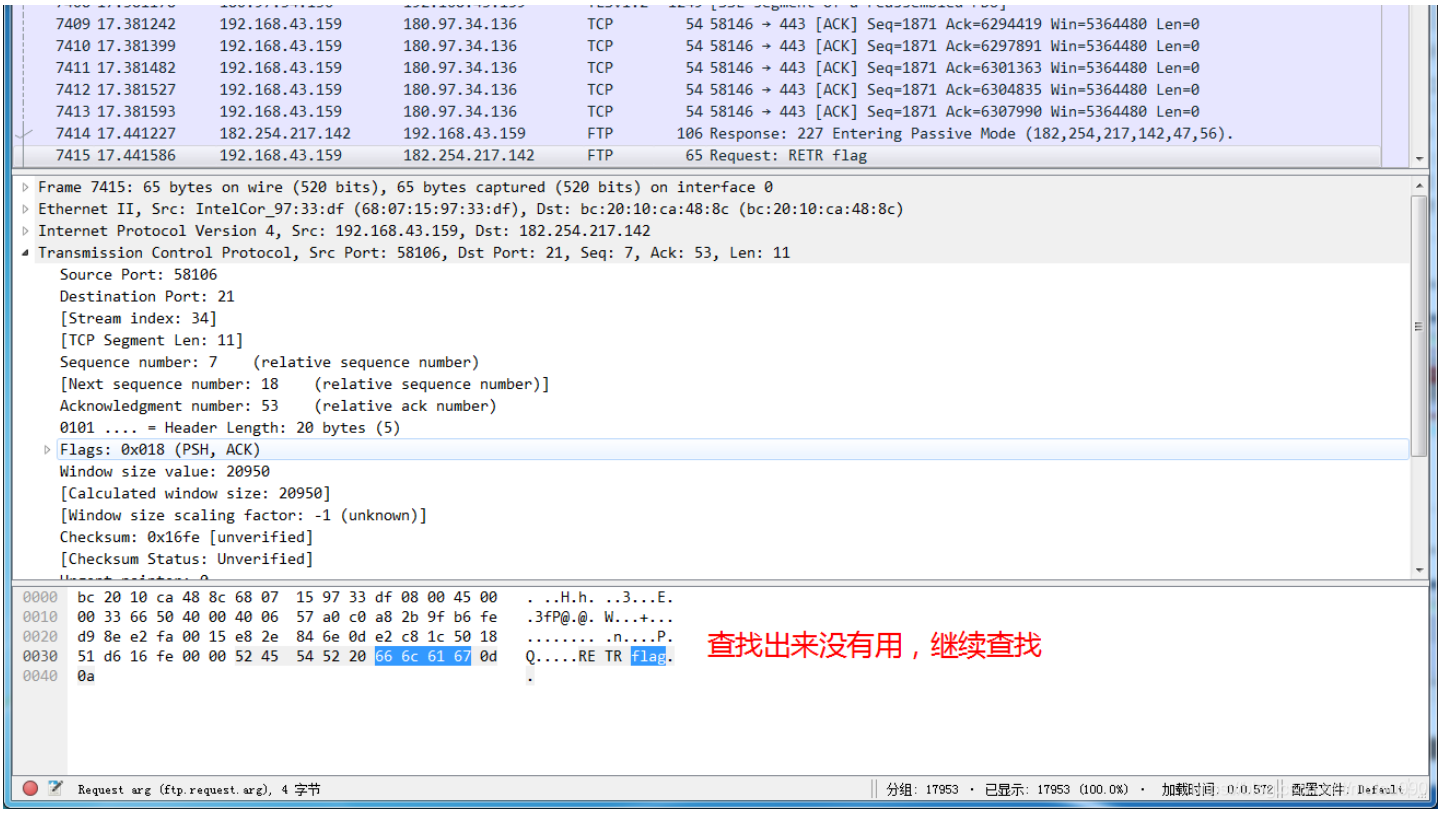


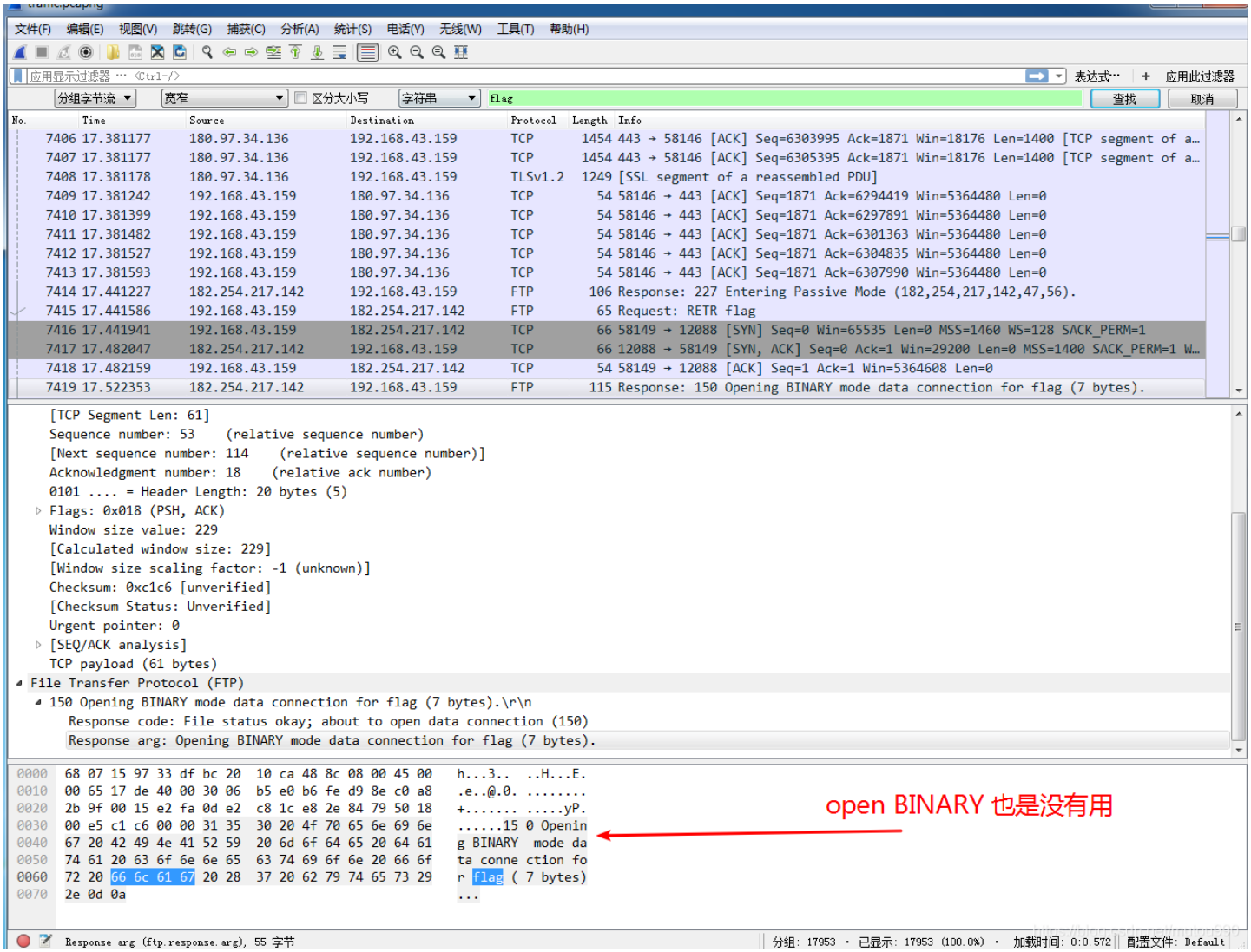


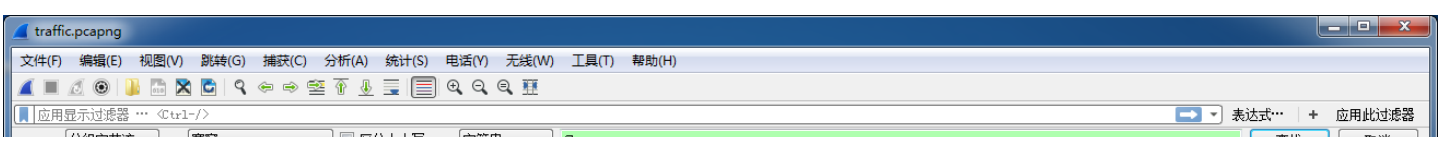
（这里可以在过滤输入框里输入FTP回车后，再对筛选过的包进行分析查看，也可以ctrl+F 查找【字符串】关键字ctrl+F 查找关键字flag或者flag的【十六进制】666c6167进行快速查找，下面直接用查找flag关键字方法）

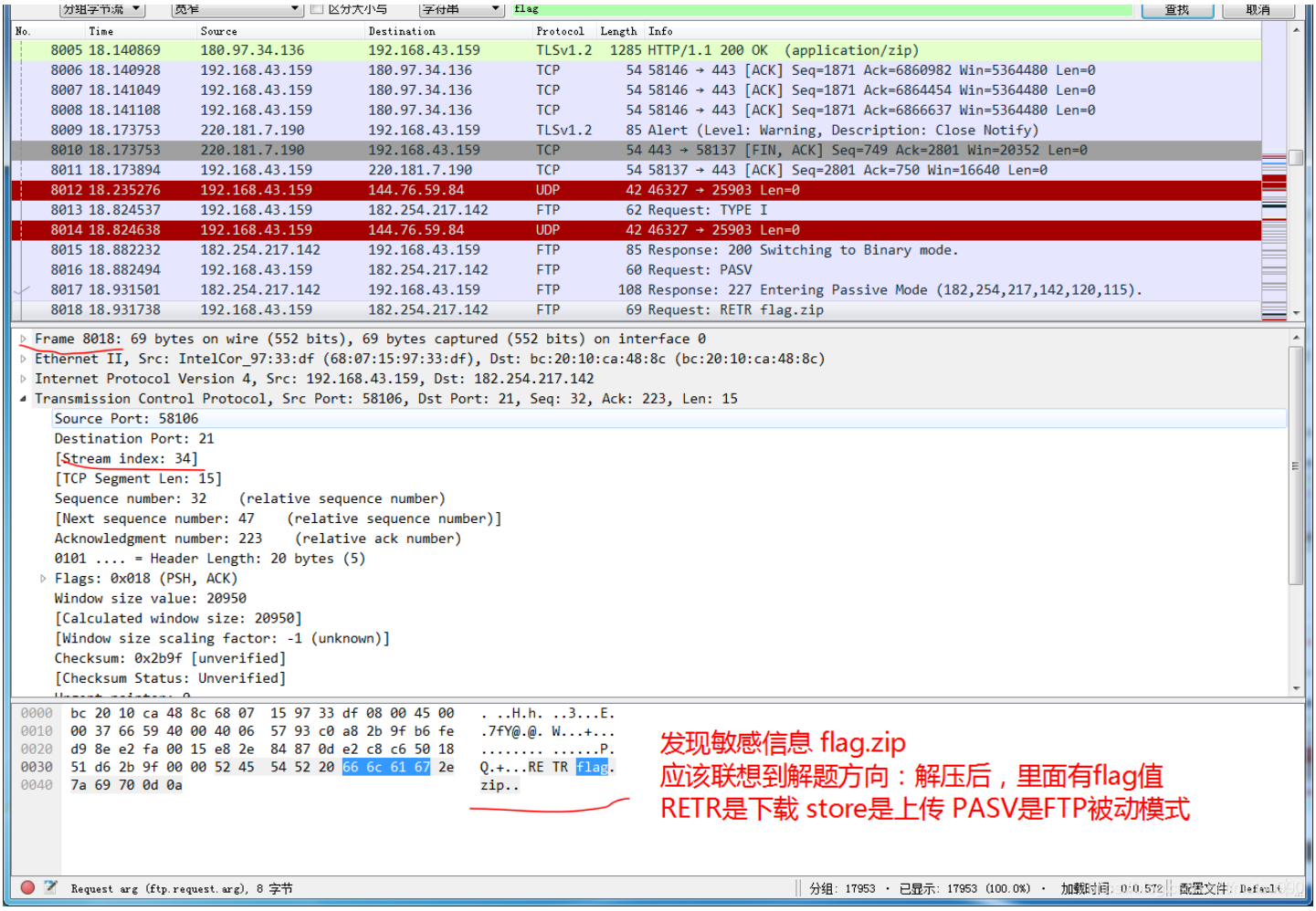




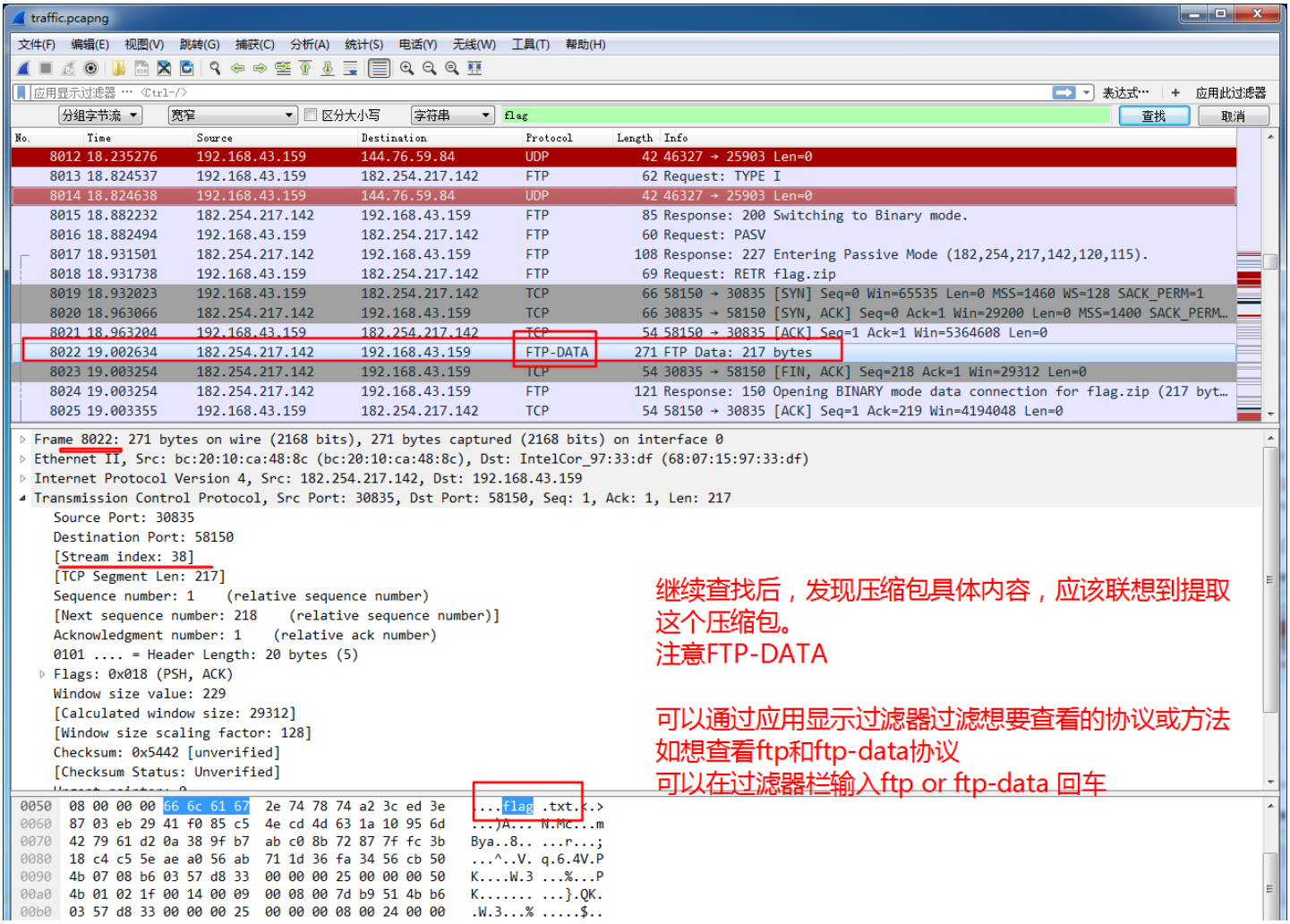

7409 17.381242 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6294419 Win=5364480 Len=0
7410 17.381399 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6297891 Win=5364480 Len=0
7411 17.381482 192.168.43.159 180.97.34.136 TCP 54 58146 → 443 [ACK] Seq=1871 Ack=6301363 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]
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
查找出来没有用，继续查找

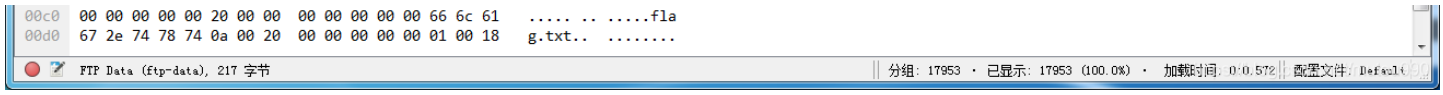

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
flag
查找
取消
No. Time Source Destination Protocol Length Info
7406 17.381177 180.97.34.136 192.168.43.159 TCP 1454 443 → 58146 [ACK] Seq=6303995 Ack=1871 Win=18176 Len=1400 [TCP segment of a…
7407 17.381177 180.97.34.136 192.168.43.159 TCP 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 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
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).
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
open BINARY 也是没有用

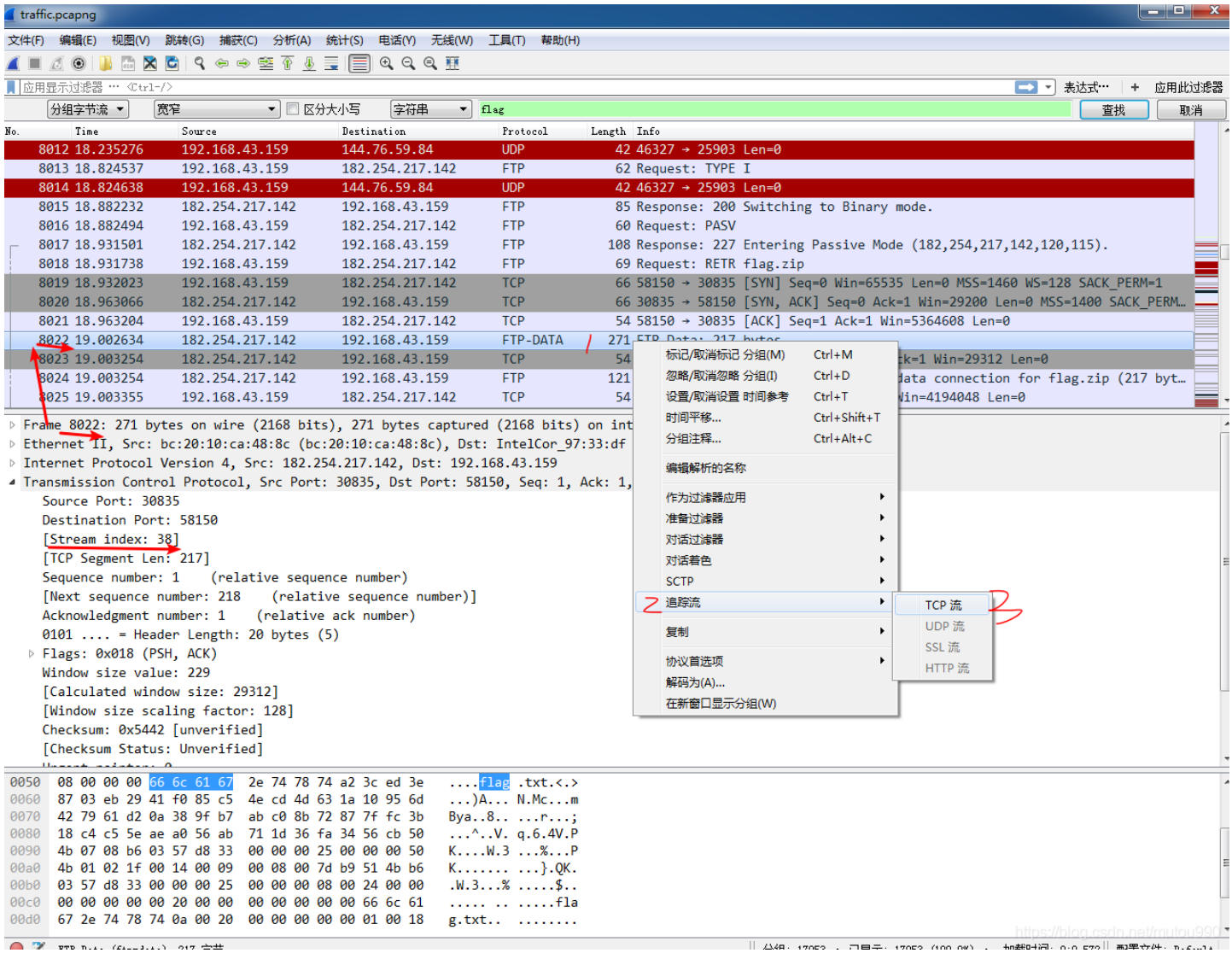

traffic.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

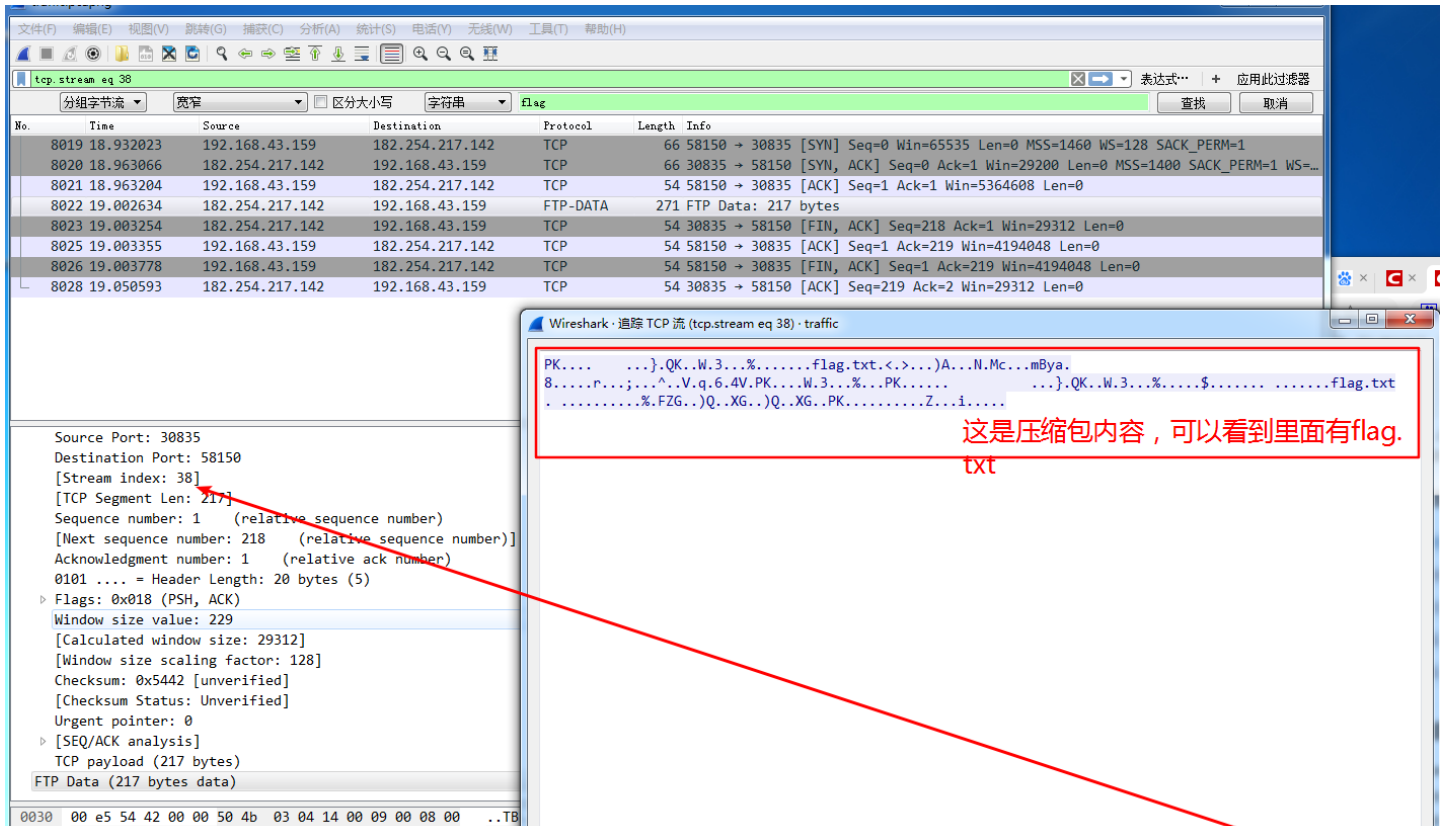


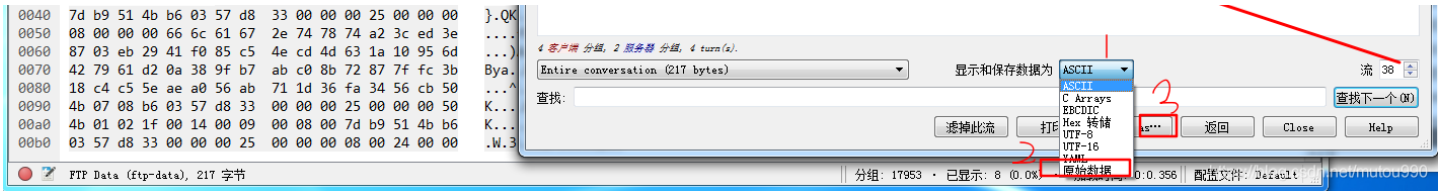
继续查找后，发现压缩包内容，如下图

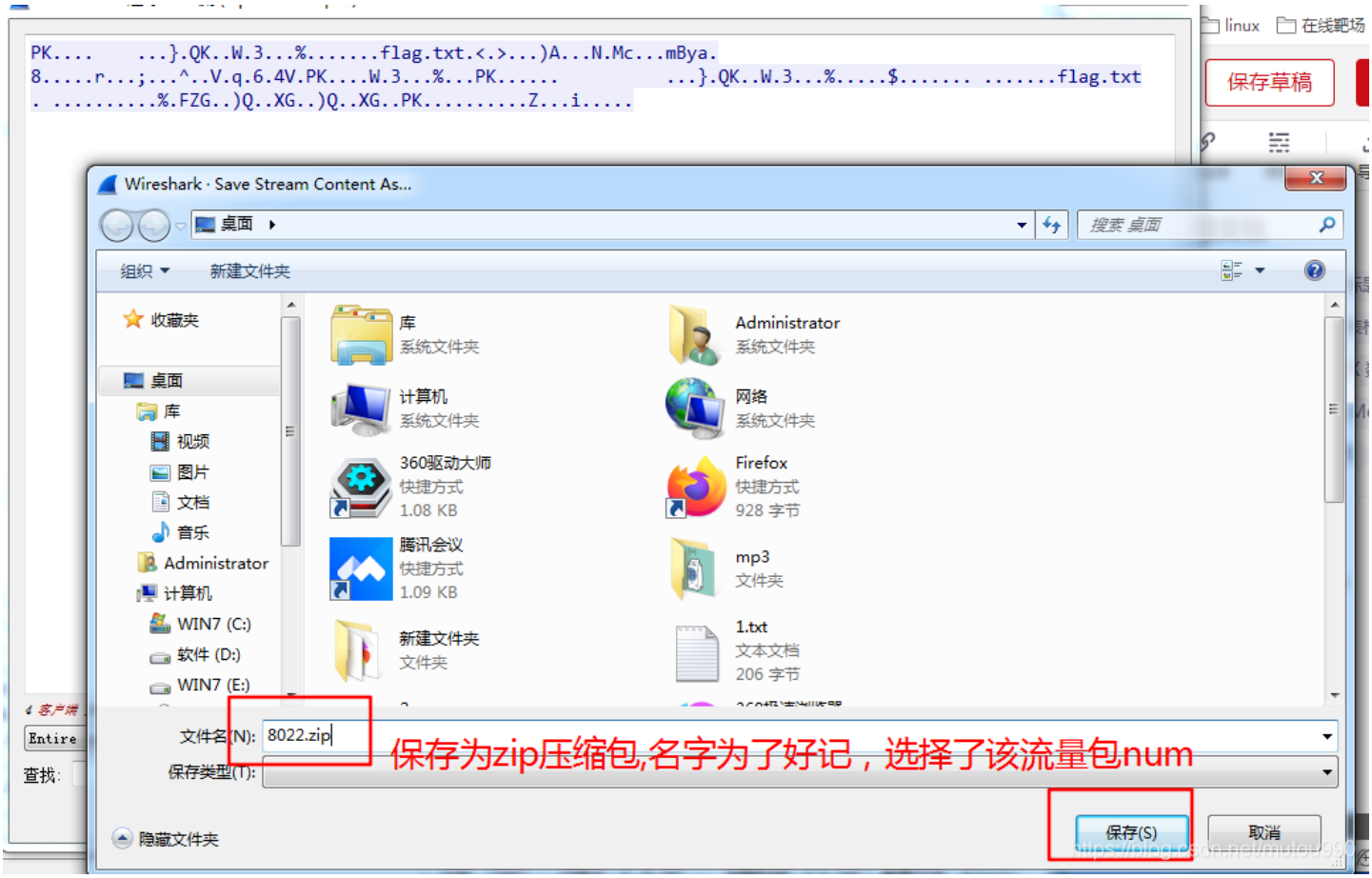


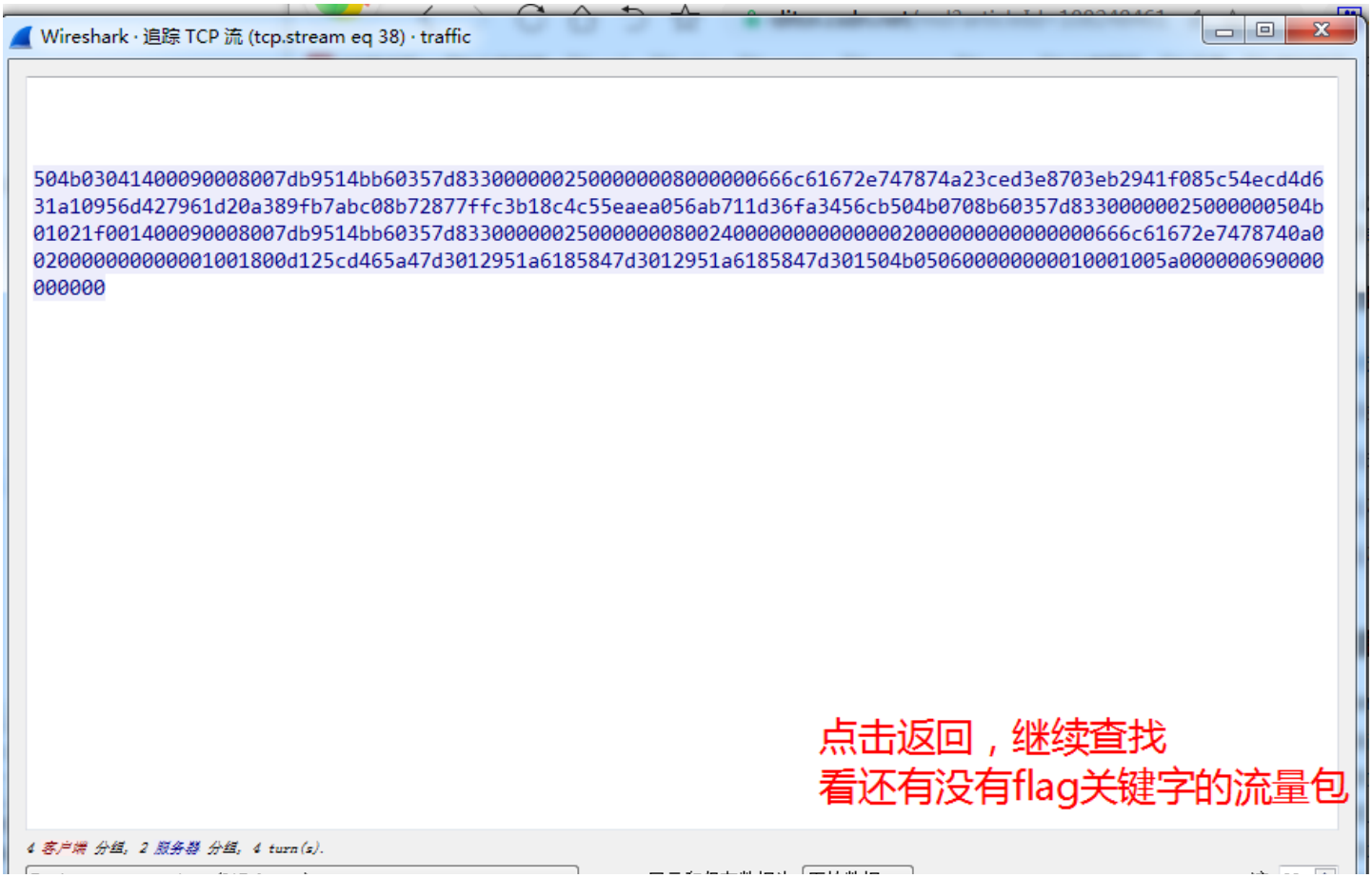

00c0 00 00 00 00 00 20 00 00 00 00 00 00 66 6c 61 ....fla
00d0 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 g.txt.. ....
FTP Data (ftp-data), 217 字节
分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.572

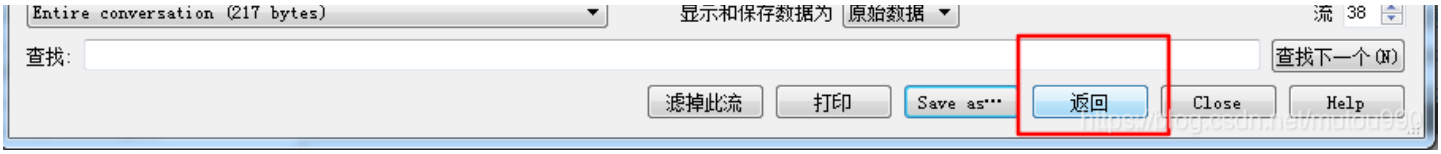

traffic.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式… 应用此过滤器
分组字节流 宽窄 区分大小写 字符串 flag 查找 取消
No. Time Source Destination Protocol Length Info
8012 18.235276 192.168.43.159 144.76.59.84 UDP 42 46327 → 25903 Len=0
8013 18.824537 192.168.43.159 182.254.217.142 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 182.254.217.142 192.168.43.159 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…
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
8024 19.003254 182.254.217.142 192.168.43.159 FTP 121
8025 19.003355 192.168.43.159 182.254.217.142 TCP 54
Frame 8022: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits) on int
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,
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]
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
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 00 25 00 00 00 08 00 24 00 00 .W.3...% .....$..
00c0 00 00 00 00 00 20 00 00 00 00 00 00 00 66 6c 61 ....fla
00d0 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 g.txt.. ....

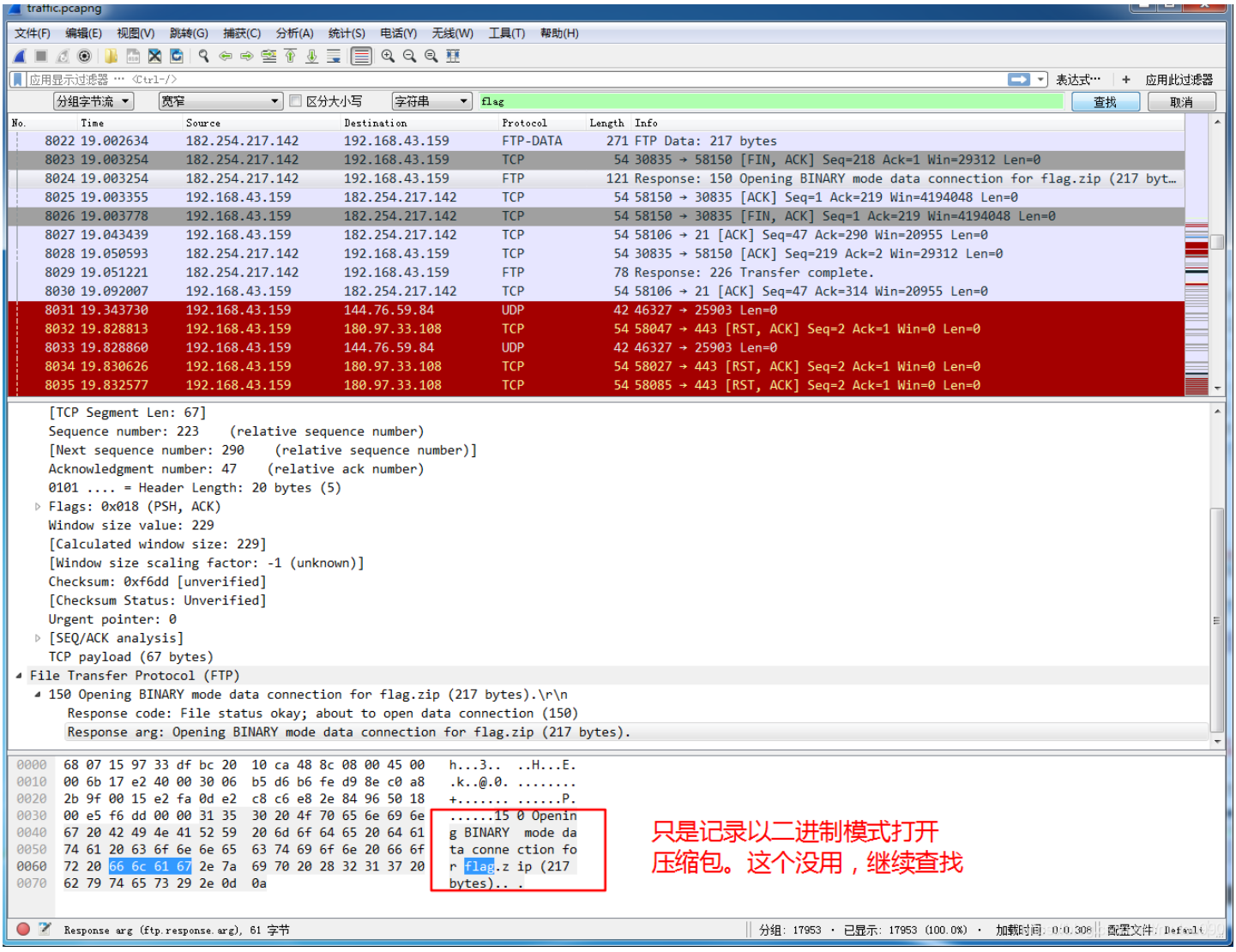

tcp.stream eq 38
No. Time Source Destination Protocol Length Info
8019 18.932023 192.168.43.159 182.254.217.142 TCP 66 58150 → 30835 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
8020 18.963066 182.254.217.142 192.168.43.159 TCP 66 30835 → 58150 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 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=218 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
Wireshark · 追踪 TCP 流 (tcp.stream eq 38) · traffic
PK.... ...}.QK..W.3...%.....flag.txt.<.>...)A...N.Mc...mBya.
8.....r...j...^..V.q.6.4V.PK....W.3...%...PK..... ...}.QK..W.3...%.....$..... .....flag.txt
. .....%.FZG..)Q..XG..)Q..XG..PK.....Z...i.....
这是压缩包内容，可以看到里面有flag.txt
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


显示和保存数据为
ASCII
Entire conversation (217 bytes)
查找:
返回
Close
Help
FTP Data (ftp-data), 217 字节

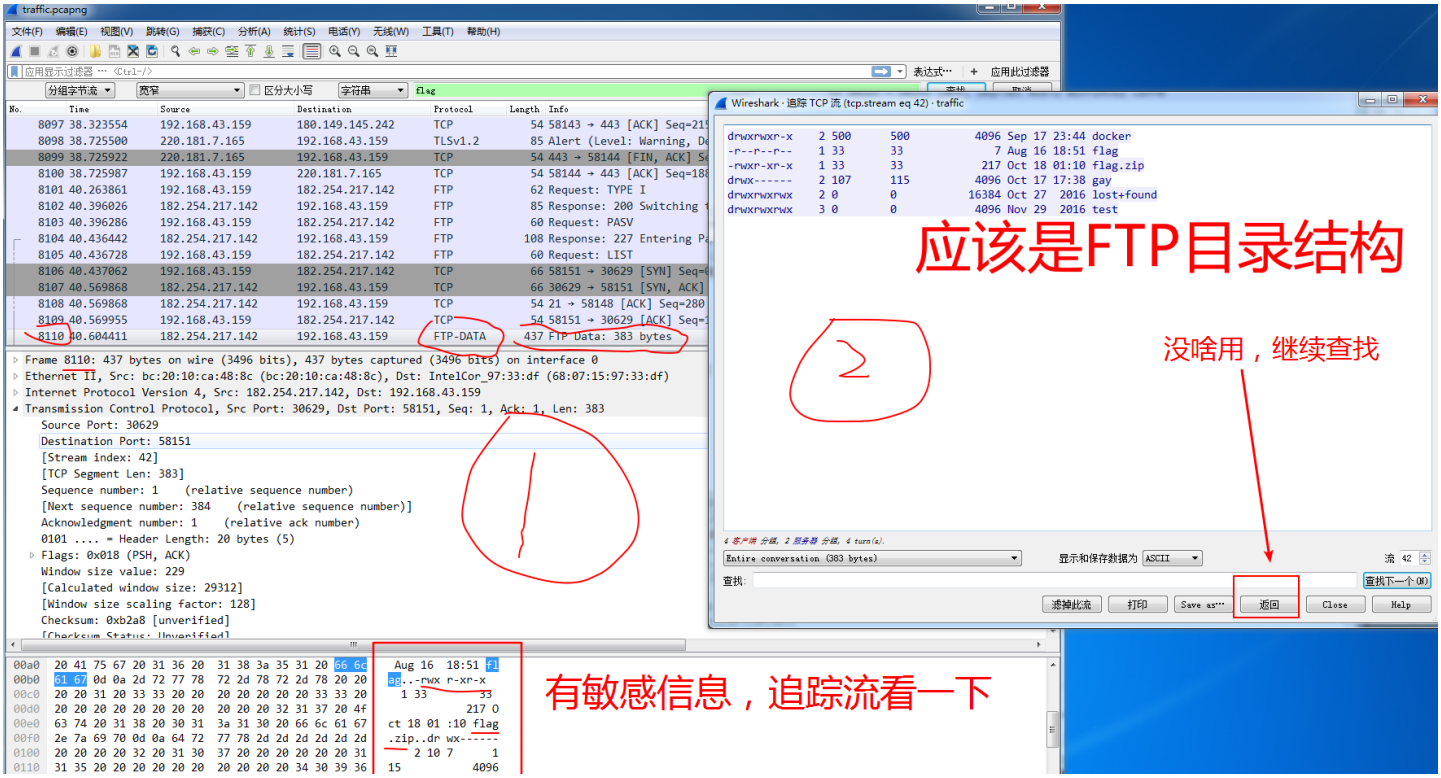

Wireshark · Save Stream Content As...
桌面
搜索 桌面
组织
新建文件夹
收藏夹
桌面
库
视频
图片
文档
音乐
Administrator
计算机
WIN7 (C:)
软件 (D:)
WIN7 (E:)
库
系统文件夹
Administrator
系统文件夹
计算机
系统文件夹
网络
系统文件夹
360驱动大师
快捷方式
1.08 KB
Firefox
快捷方式
928 字节
腾讯会议
快捷方式
1.09 KB
mp3
文件夹
新建文件夹
文件夹
1.txt
文本文档
206 字节
文件名(N): 8022.zip
保存类型(T):
保存(S)
取消
隐藏文件夹
保存为zip压缩包,名字为了好记，选择了该流量包num


Wireshark · 追踪 TCP 流 (tcp.stream eq 38) · traffic
504b0304140009000800 7db9514bb60357d8330000002500000008000000666c61672e747874a23ced3e8703eb2941f085c54ecd4d631a10956d427961d20a389fb7abc08b72877ffc3b18c4c55eaea056ab711d36fa3456cb504b0708b60357d8330000002500000050 4b01021f00140009000800 7db9514bb60357d8330000002500000008002400000000000000200000000000000000666c61672e7478740a0020000000000001001800d125cd465a47d3012951a6185847d3012951a6185847d301504b0506000000000100010050000000690000000000
点击返回，继续查找
看还有没有flag关键字的流量包





只是记录以二进制模式打开
压缩包。这个没用，继续查找

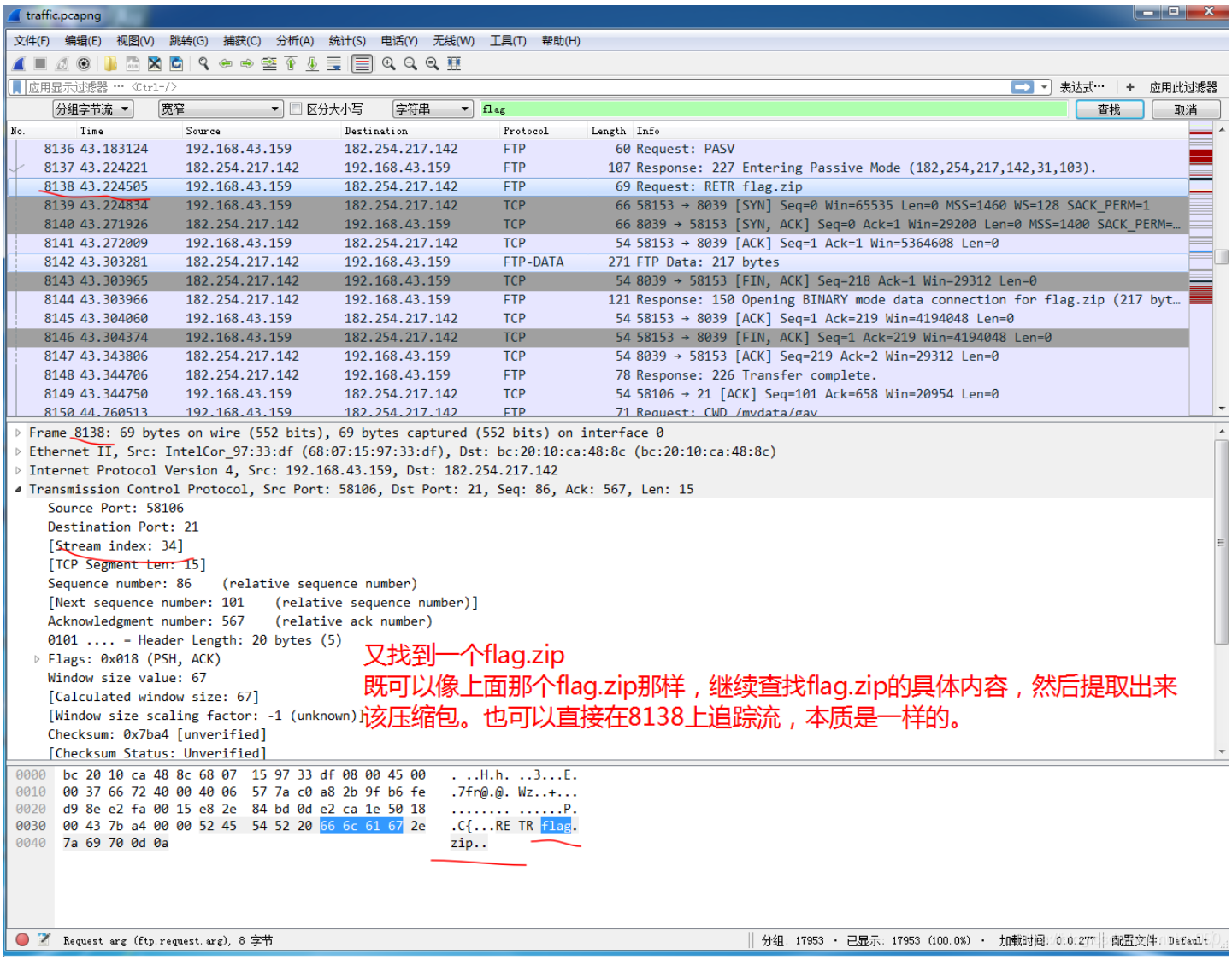


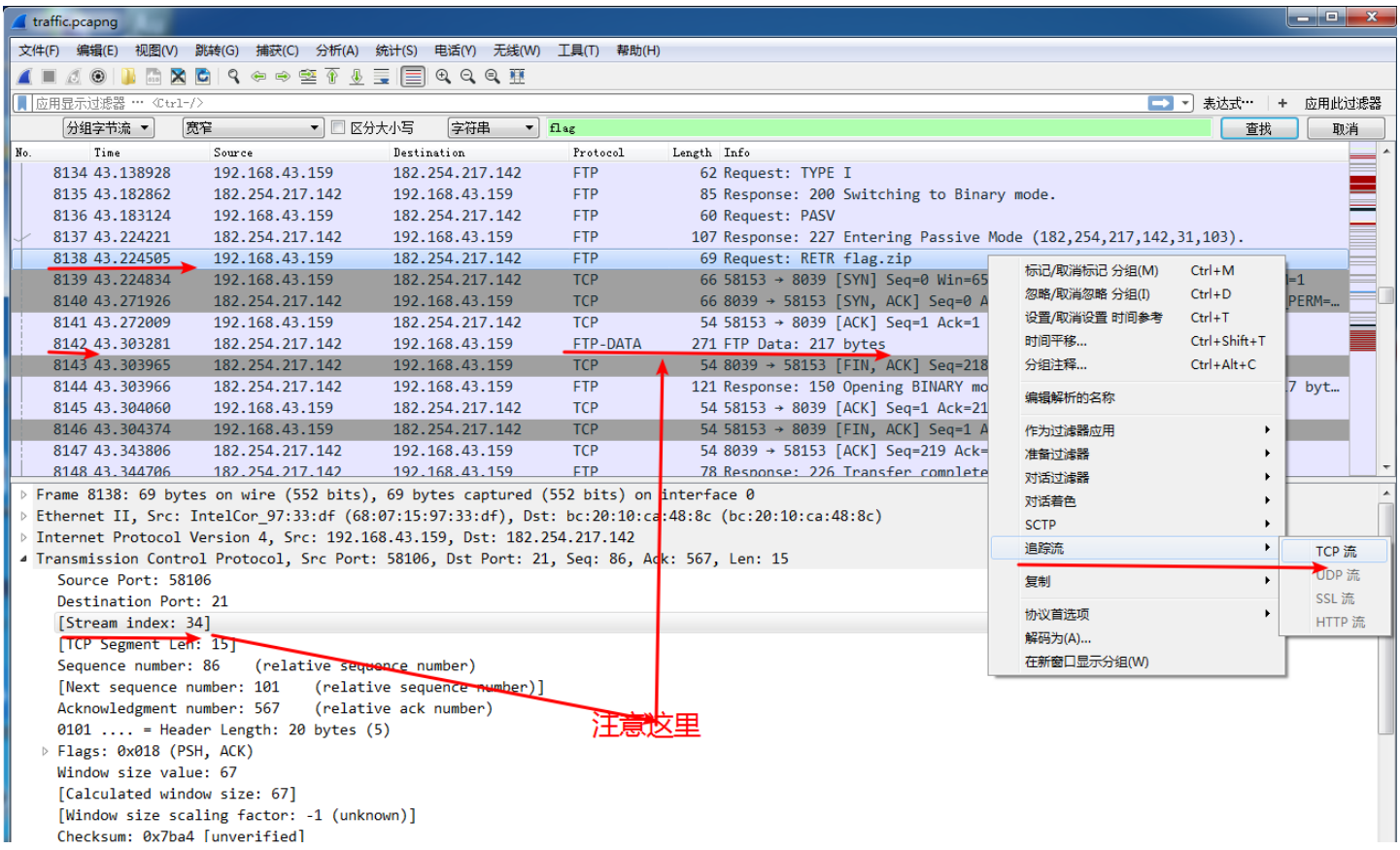
应该是FTP目录结构

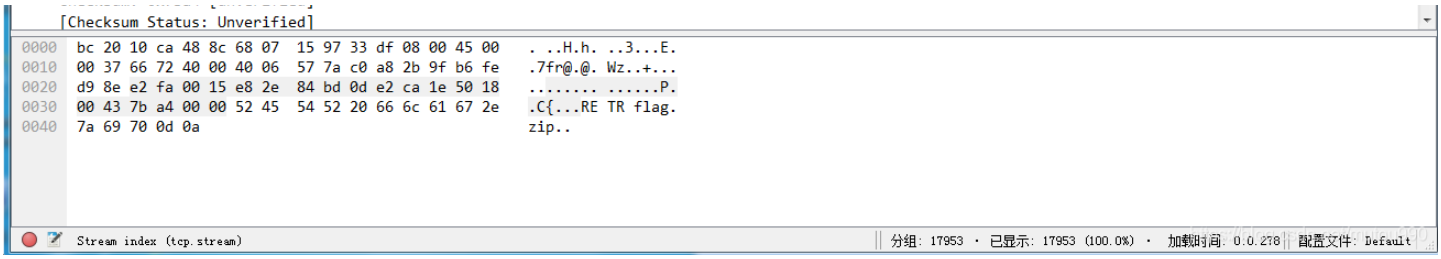
没啥用，继续查找

有敏感信息，追踪流看一下

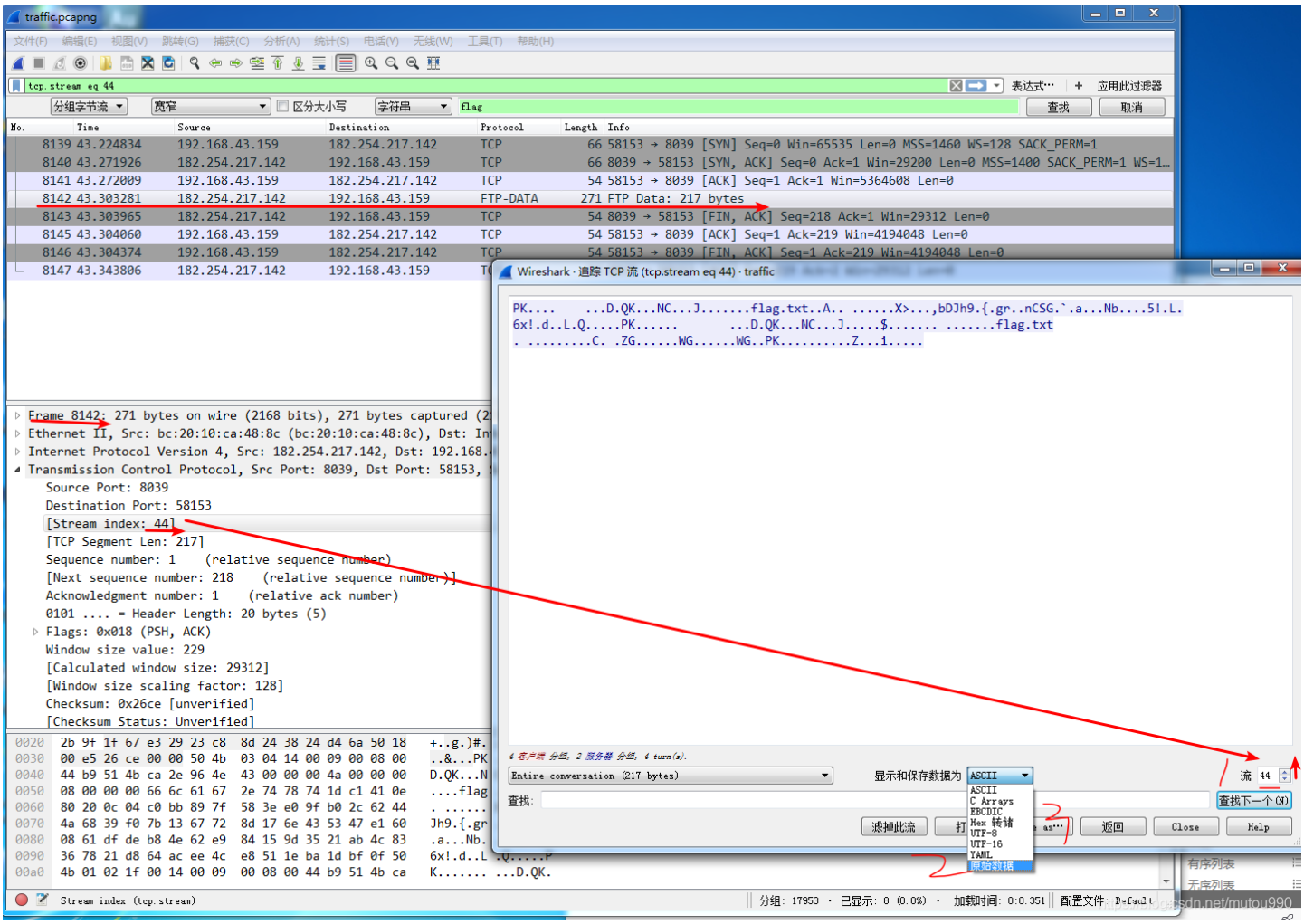

0120 20 4f 63 74 20 31 37 20 31 37 3a 33 38 20 67 61
Oct 17 17:38 ga
FTP Data (ftp-data), 383 字节
分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.308 配置文件: Default
https://blog.csdn.net/mutou990

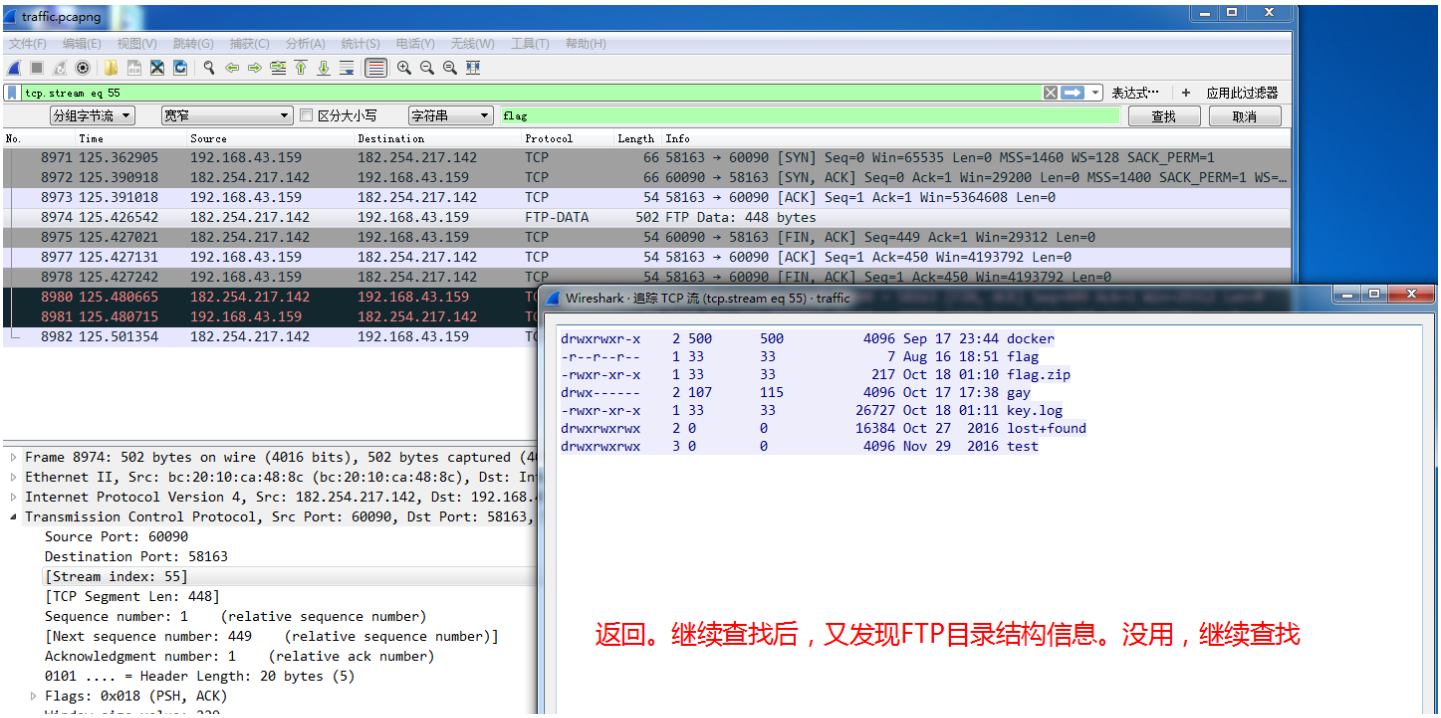

traffic.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式… 应用此过滤器
分组字节流 宽窄 区分大小写 字符串 flag 查找 取消
No. Time Source Destination Protocol Length Info
8136 43.183124 192.168.43.159 182.254.217.142 FTP 60 Request: PASV
8137 43.224221 182.254.217.142 192.168.43.159 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=…
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 /mydata/gav
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]
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。
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

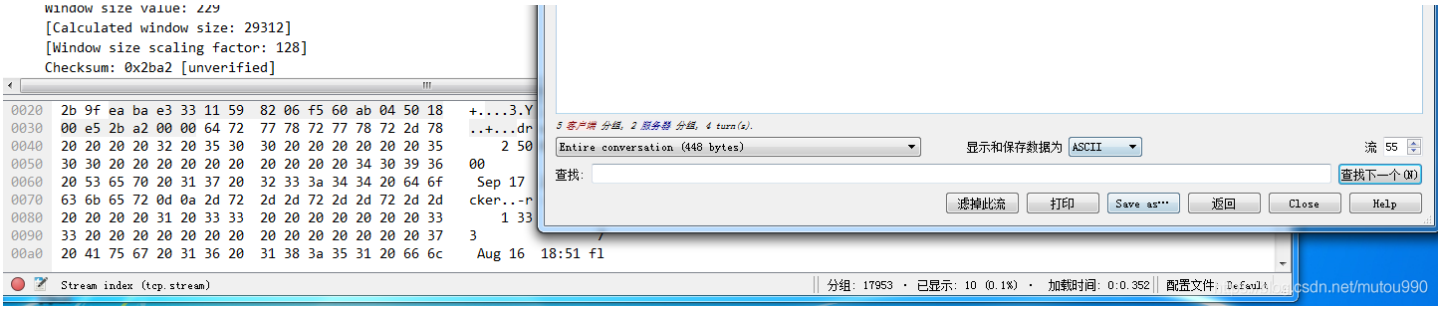

traffic.pcapng
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式… 应用此过滤器
分组字节流 宽窄 区分大小写 字符串 flag 查找 取消
No. Time Source Destination Protocol Length Info
8134 43.138928 192.168.43.159 182.254.217.142 FTP 62 Request: TYPE I
8135 43.182862 182.254.217.142 192.168.43.159 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=65
8140 43.271926 182.254.217.142 192.168.43.159 TCP 66 8039 → 58153 [SYN, ACK] Seq=0 A
8141 43.272009 192.168.43.159 182.254.217.142 TCP 54 58153 → 8039 [ACK] Seq=1 Ack=1
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
8144 43.303966 182.254.217.142 192.168.43.159 FTP 121 Response: 150 Opening BINARY mo
8145 43.304060 192.168.43.159 182.254.217.142 TCP 54 58153 → 8039 [ACK] Seq=1 Ack=21
8146 43.304374 192.168.43.159 182.254.217.142 TCP 54 58153 → 8039 [FIN, ACK] Seq=1 A
8147 43.343806 182.254.217.142 192.168.43.159 TCP 54 8039 → 58153 [ACK] Seq=219 Ack=
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


[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..
Stream index (tcp.stream)
分组: 17953 · 已显示: 17953 (100.0%) · 加载时间: 0:0.278 配置文件: Default

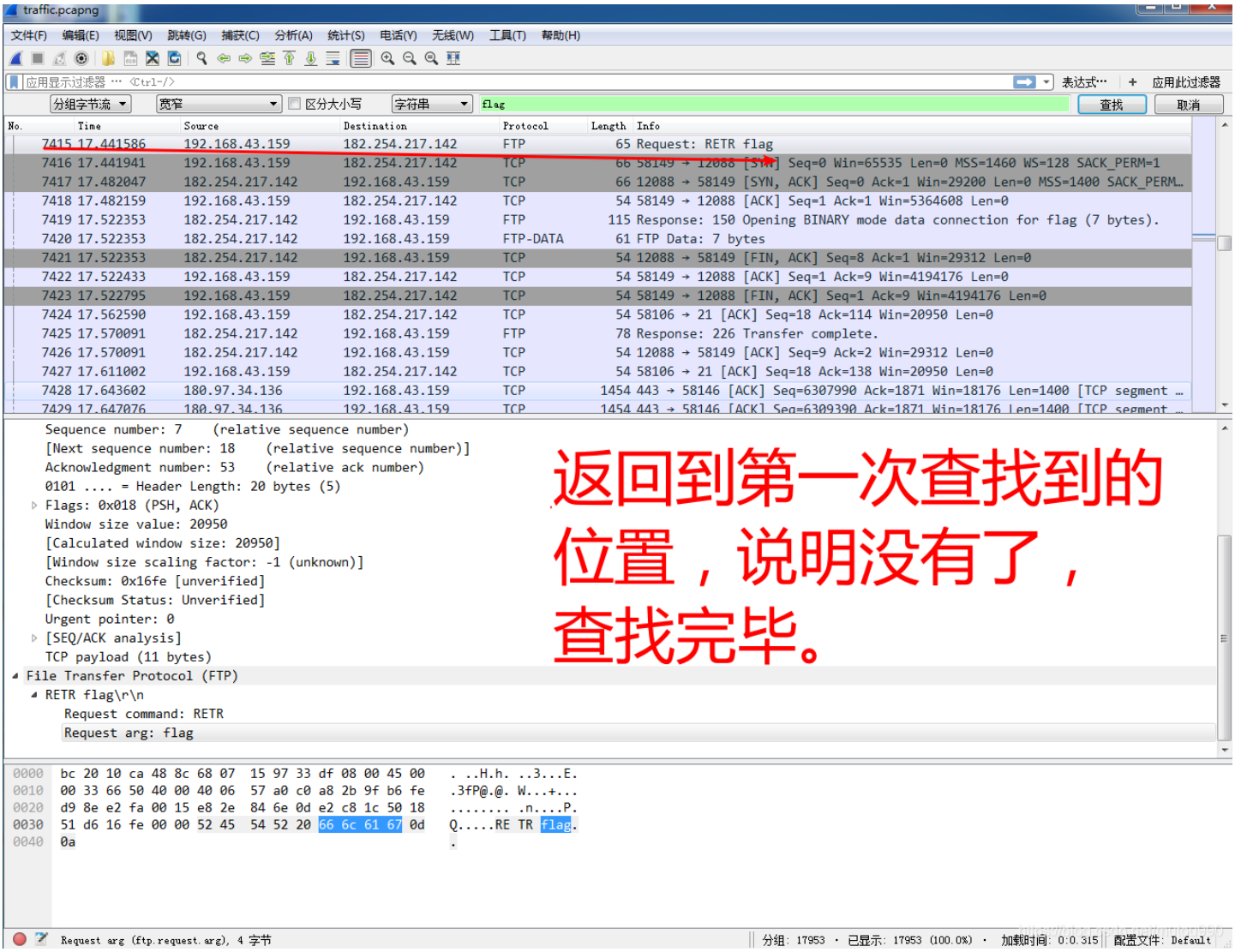
点击流的向上按钮


traffic.pcapng
tcp.stream eq 44
No. Time Source Destination Protocol Length Info
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 WS=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
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 TC
Wireshark · 追踪 TCP 流 (tcp.stream eq 44) · traffic
PK.... ...D.QK...NC...J.....flag.txt..A.. .....X>...,bDJh9.{.gr..nCSG.`.a...Nb....5!.L.
6x!.d..L.Q.....PK..... ...D.QK...NC...J.....$..... .....flag.txt
. .....C. .ZG.....WG.....WG..PK.....Z...i.....
Frame 8142: 271 bytes on wire (2168 bits), 271 bytes captured (2
Ethernet II, Src: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c), Dst: In
Internet Protocol Version 4, Src: 182.254.217.142, Dst: 192.168.
Transmission Control Protocol, Src Port: 8039, Dst Port: 58153,
Source Port: 8039
Destination Port: 58153
[Stream index: 44]
[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: 0x26ce [unverified]
[Checksum Status: Unverified]
0020 2b 9f 1f 67 e3 29 23 c8 8d 24 38 24 d4 6a 50 18 +..g.)#. .8.jP.
0030 00 e5 26 ce 00 00 50 4b 03 04 14 00 09 00 08 00 ..&...PK ....
0040 44 b9 51 4b ca 2e 96 4e 43 00 00 00 4a 00 00 00 D.QK...N C...J...
0050 08 00 00 00 66 6c 61 67 2e 74 78 74 1d c1 41 0e ....flag .txt..A.
0060 80 20 0c 04 c0 bb 89 7f 58 3e e0 9f b0 2c 62 44 . ..... X>...,bD
0070 4a 68 39 f0 7b 13 67 72 8d 17 6e 43 53 47 e1 60 Jh9.{.gr ..nCSG.`
0080 08 61 df de b8 4e 62 e9 84 15 9d 35 21 ab 4c 83 .a...Nb. ..5!.L.
0090 36 78 21 d8 64 ac ee 4c e8 51 1e ba 1d bf 0f 50 6x!.d..L .Q.....P
00a0 4b 01 02 1f 00 14 00 09 00 08 00 44 b9 51 4b ca K..... ...D.QK.
4 客户端 分组, 2 服务器 分组, 4 turn(s).
Entire conversation (217 bytes)
显示和保存数据为 ASCII
ASCII
C Arrays
EBCDIC
Hex 转储
UTF-8
UTF-16
YAML
原始数据
流 44
查找:
查找下一个 (N)
滤掉此流
返回
Close
Help
Stream index (tcp.stream)
分组: 17953 · 已显示: 8 (0.0%) · 加载时间: 0:0.351 配置文件: Default

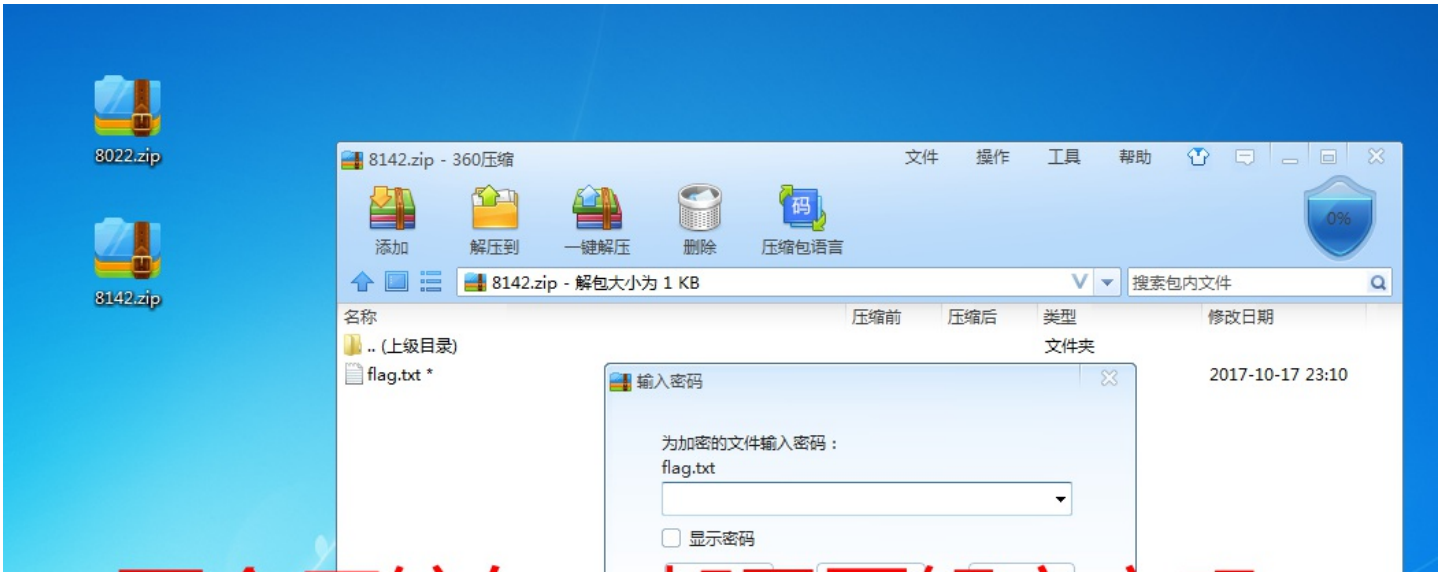

traffic.pcapng
tcp.stream eq 55
No. Time Source Destination Protocol Length Info
8971 125.362905 192.168.43.159 182.254.217.142 TCP 66 58163 → 60090 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
8972 125.390918 182.254.217.142 192.168.43.159 TCP 66 60090 → 58163 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM=1 WS=…
8973 125.391018 192.168.43.159 182.254.217.142 TCP 54 58163 → 60090 [ACK] Seq=1 Ack=1 Win=5364608 Len=0
8974 125.426542 182.254.217.142 192.168.43.159 FTP-DATA 502 FTP Data: 448 bytes
8975 125.427021 182.254.217.142 192.168.43.159 TCP 54 60090 → 58163 [FIN, ACK] Seq=449 Ack=1 Win=29312 Len=0
8977 125.427131 192.168.43.159 182.254.217.142 TCP 54 58163 → 60090 [ACK] Seq=1 Ack=450 Win=4193792 Len=0
8978 125.427242 192.168.43.159 182.254.217.142 TCP 54 58163 → 60090 [FIN, ACK] Seq=1 Ack=450 Win=4193792 Len=0
8980 125.480665 182.254.217.142 192.168.43.159 TC
8981 125.480715 192.168.43.159 182.254.217.142 TC
8982 125.501354 182.254.217.142 192.168.43.159 TC
Wireshark · 追踪 TCP 流 (tcp.stream eq 55) · traffic
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
Frame 8974: 502 bytes on wire (4016 bits), 502 bytes captured (4
Ethernet II, Src: bc:20:10:ca:48:8c (bc:20:10:ca:48:8c), Dst: In
Internet Protocol Version 4, Src: 182.254.217.142, Dst: 192.168.
Transmission Control Protocol, Src Port: 60090, Dst Port: 58163,
Source Port: 60090
Destination Port: 58163
[Stream index: 55]
[TCP Segment Len: 448]
Sequence number: 1 (relative sequence number)
[Next sequence number: 449 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
返回。继续查找后，又发现FTP目录结构信息。没用，继续查找

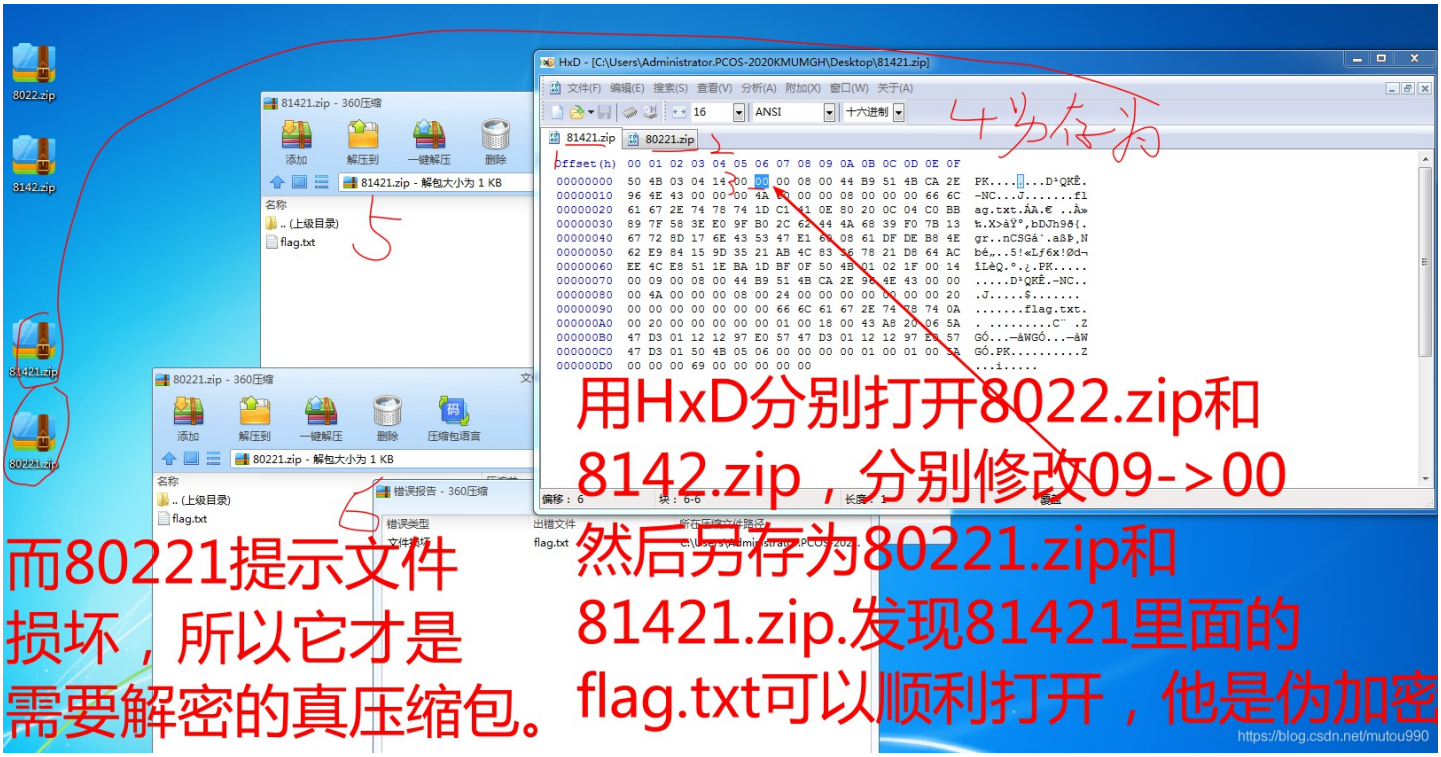


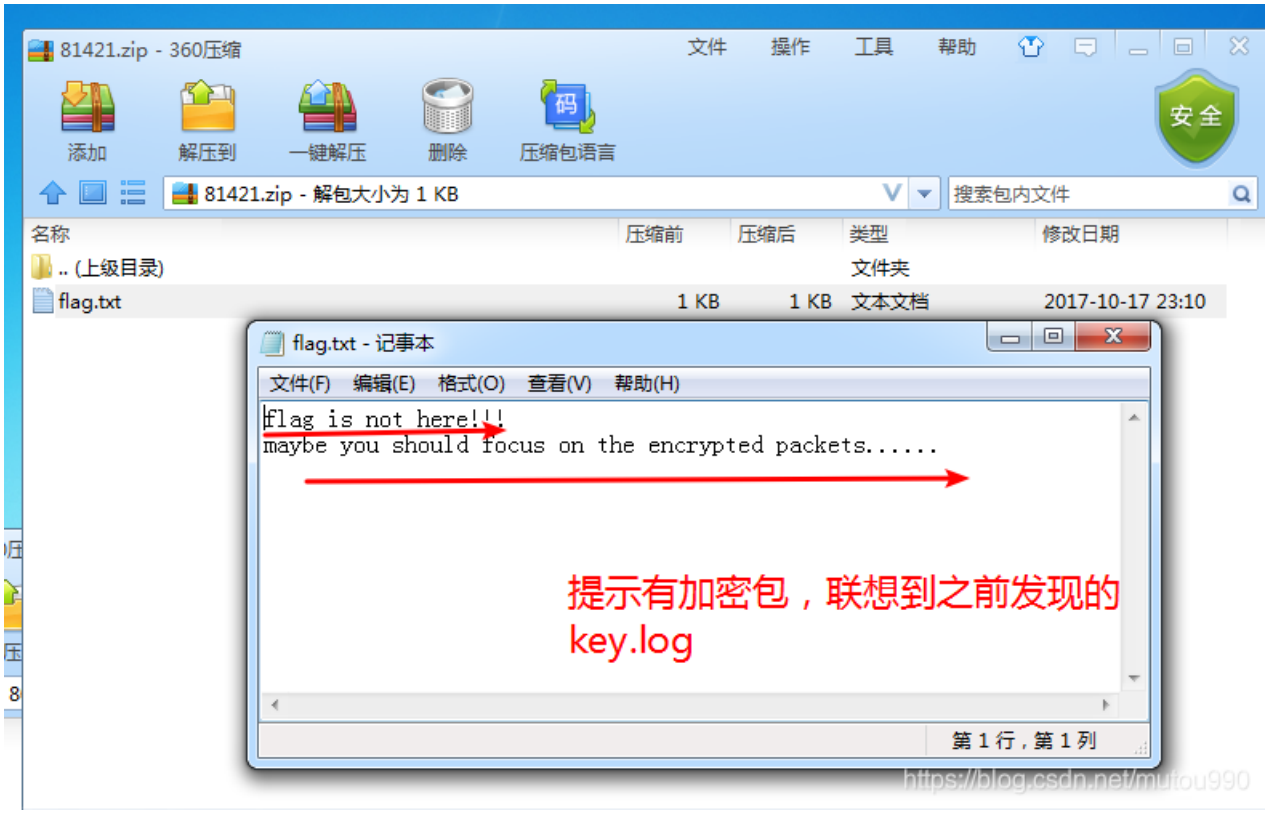
注意这里有一个key.log文件



返回到第一次查找到的位置，说明没有了，查找完毕。

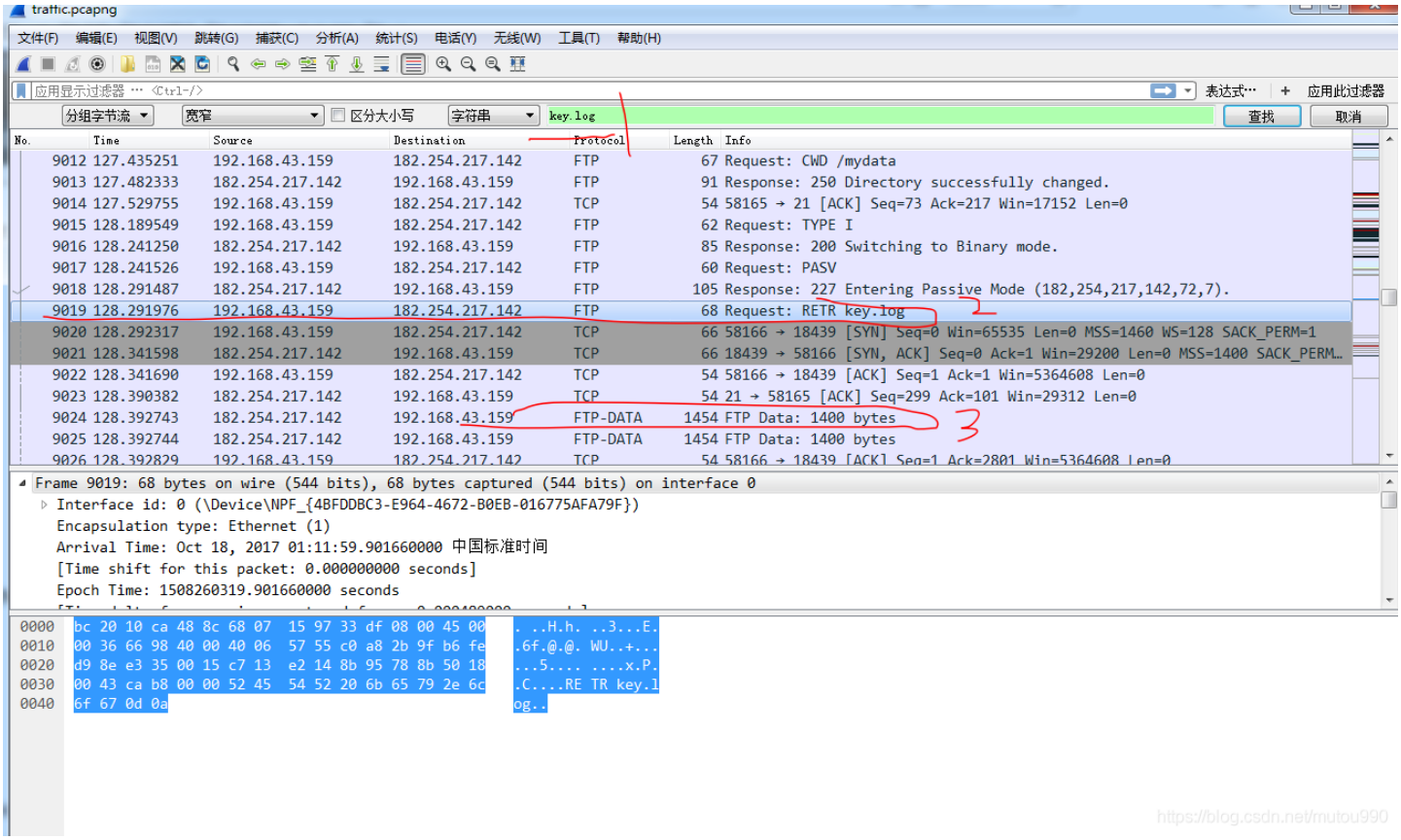


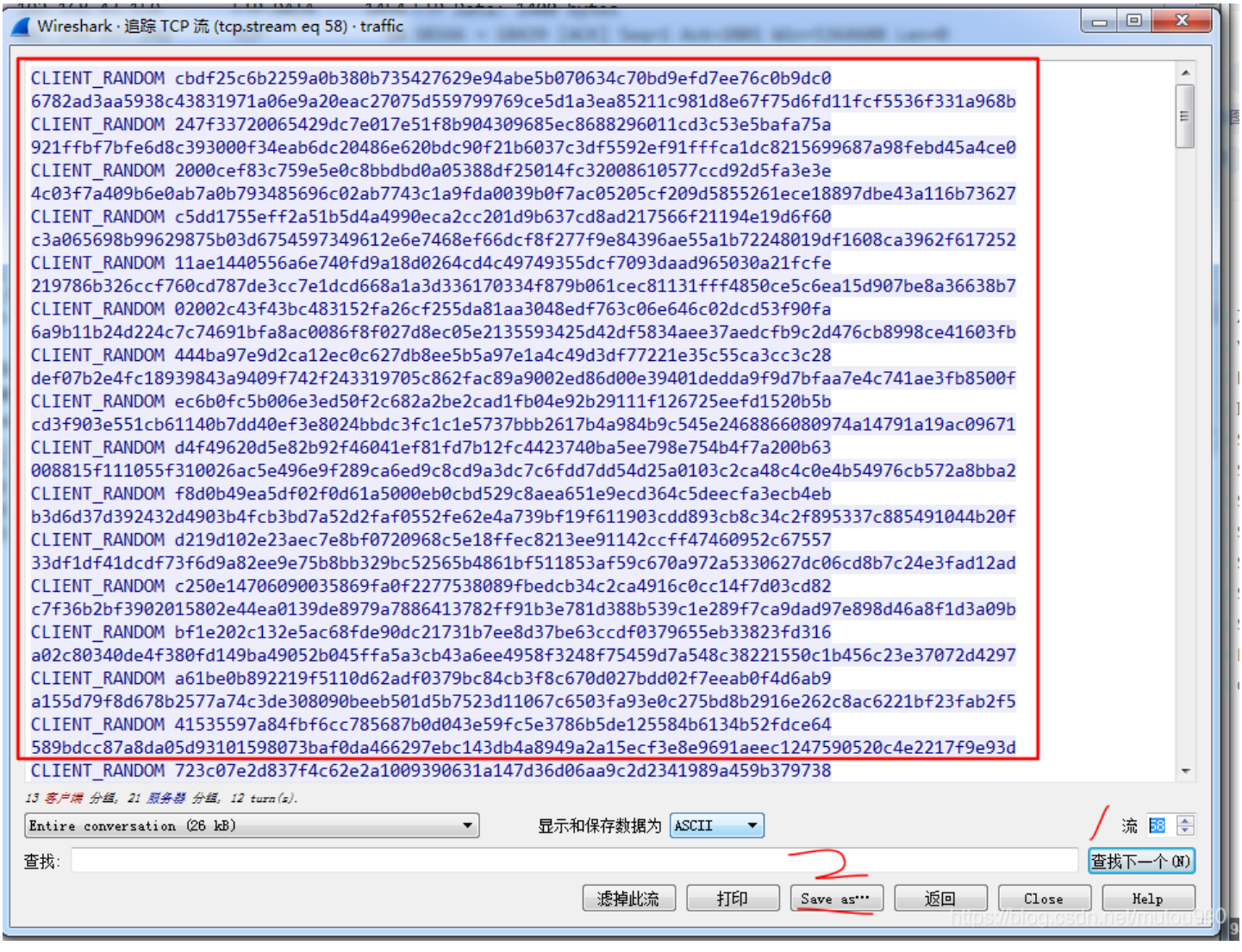




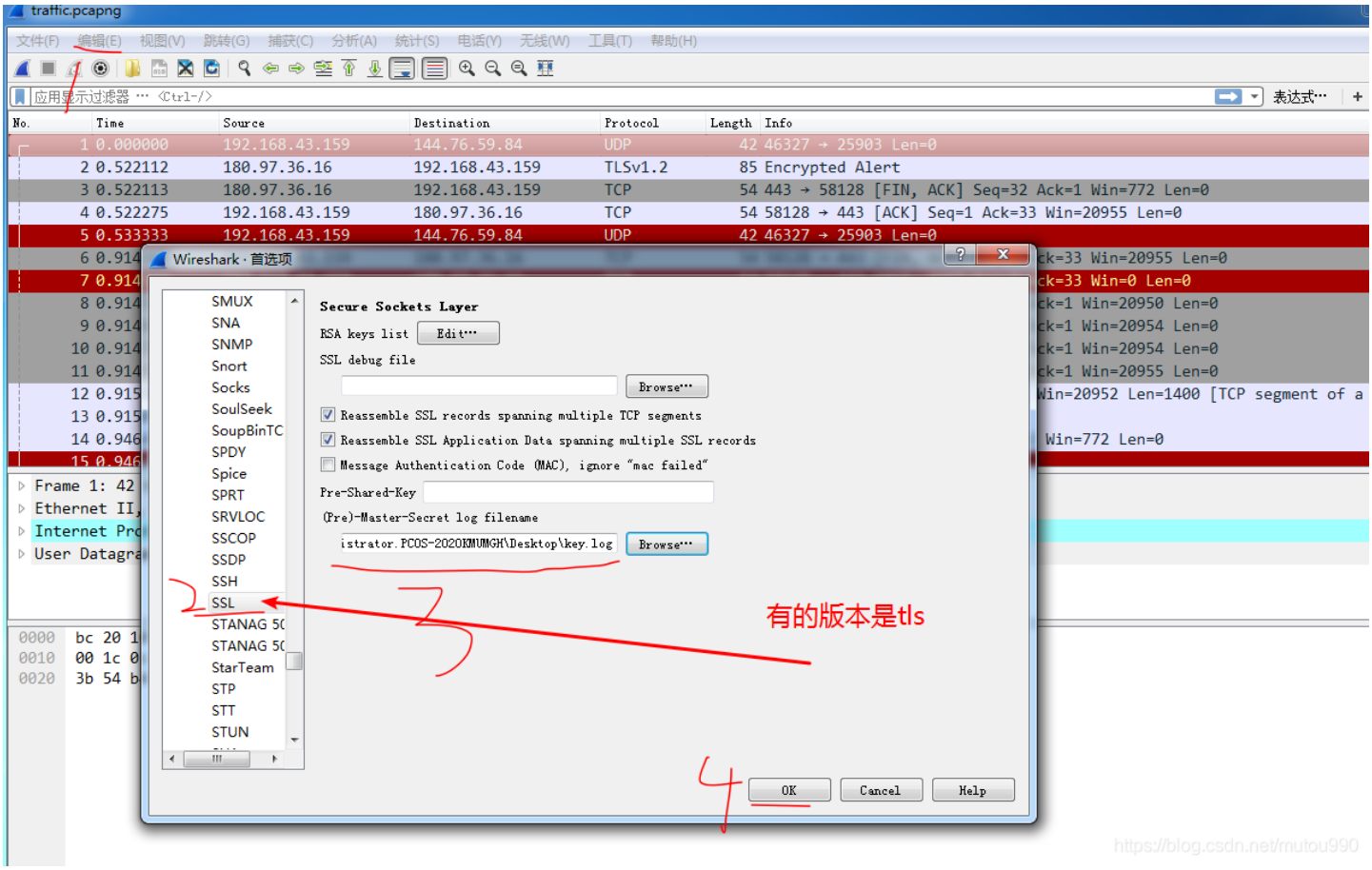
解密后从压缩包中提取到了一个flag.txt，打开发现是假的flag，并提示“maybe you should focus on the encrypted packets…”，意思是“也许你应该关注加密的数据包…”

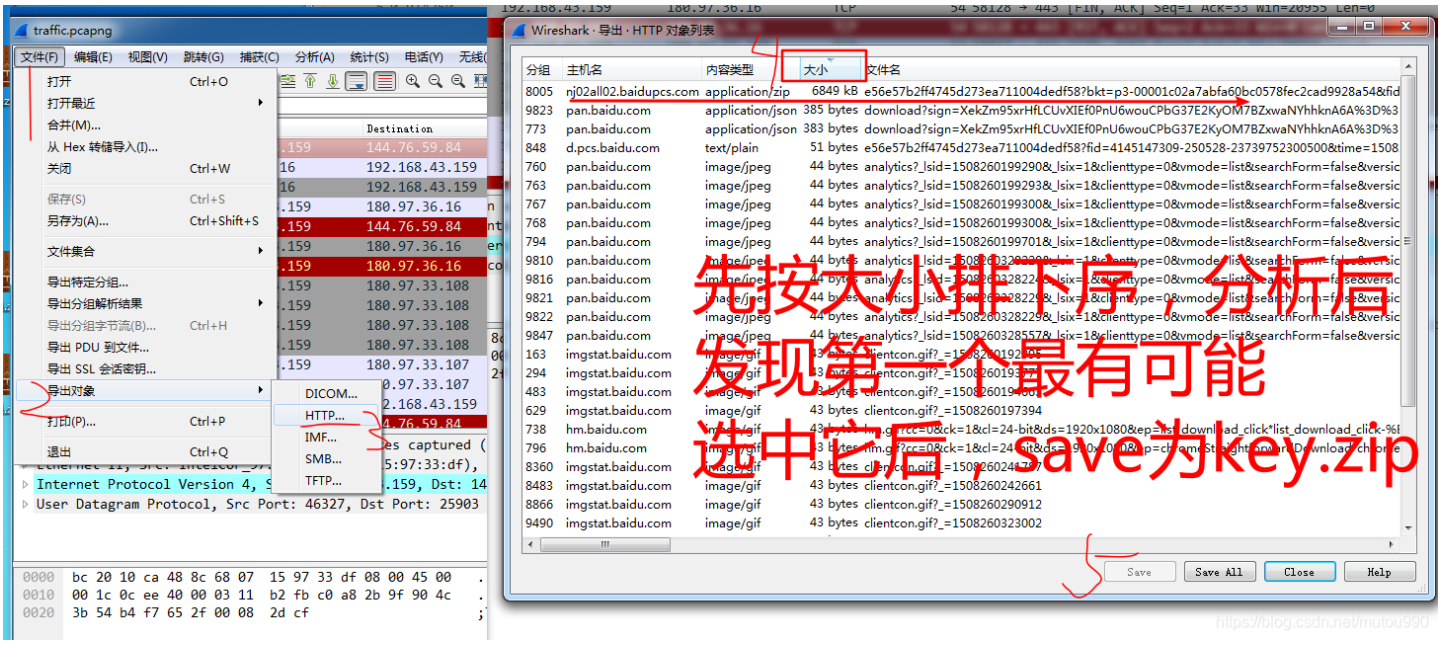
下面提取key.log文件

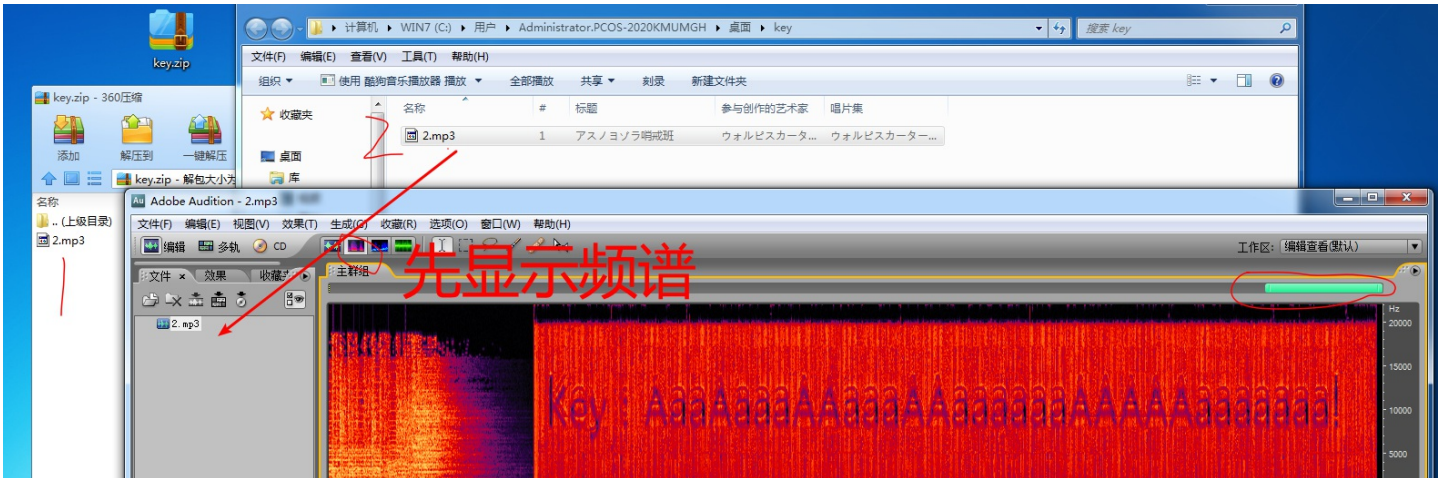




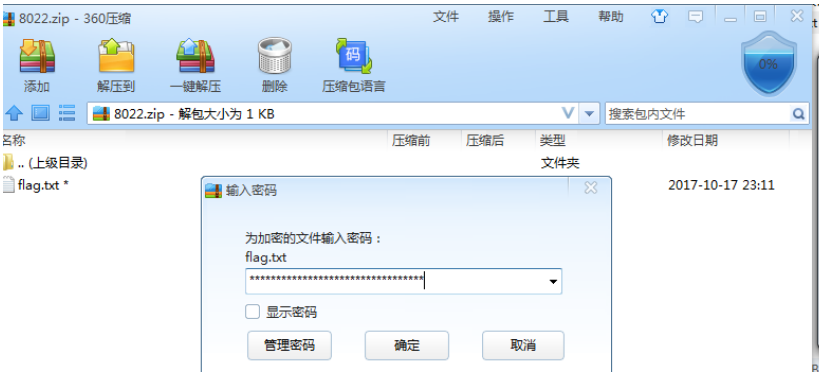
加密的数据包？那就应该是TLS协议没跑了，又想到key.log这个文件还没有用，然后使用key.log对TLS协议进行解密。（操作步骤：编辑→首选项→Protocols→TLS，然后在下面导入key.log文件）

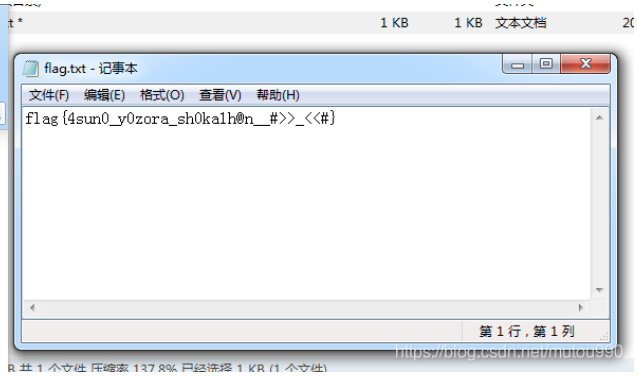

traffic.pcapng
Wireshark · 首选项
Secure Sockets Layer
RSA keys list
Edit···
SSL debug file
Browse···
Reassemble SSL records spanning multiple TCP segments
Reassemble SSL Application Data spanning multiple SSL records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared-Key
(Pre)-Master-Secret log filename
SSL
有的版本是tls
OK
Cancel
Help


traffic.pcapng
Wireshark · 导出 · HTTP 对象列表
DICOM...
HTTP...
IMF...
SMB...
TFTP...
先按文件->导出对象->HTTP
发现第一个最有可能
选中后点save为key.zip
Save
Save All
Close
Help


key.zip
Adobe Audition - 2.mp3
先显示频谱
Key : AaaAaaaAAaaaAAaaaaaaAAAAAaaaaaaa!

直接把该key提交flag,先试试，发现不对。那就解密压缩包

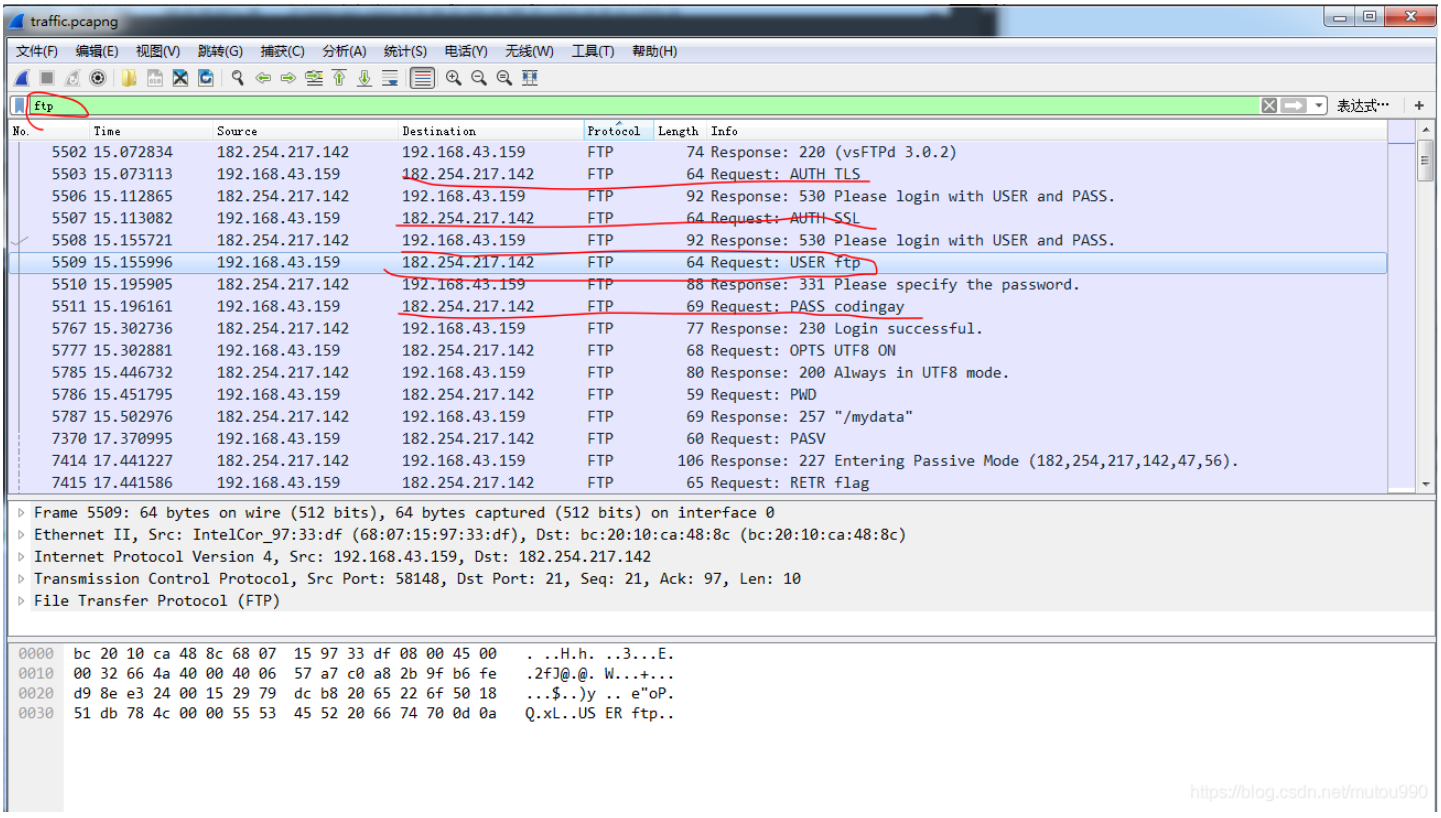




成功！

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协议是由用的，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）

。

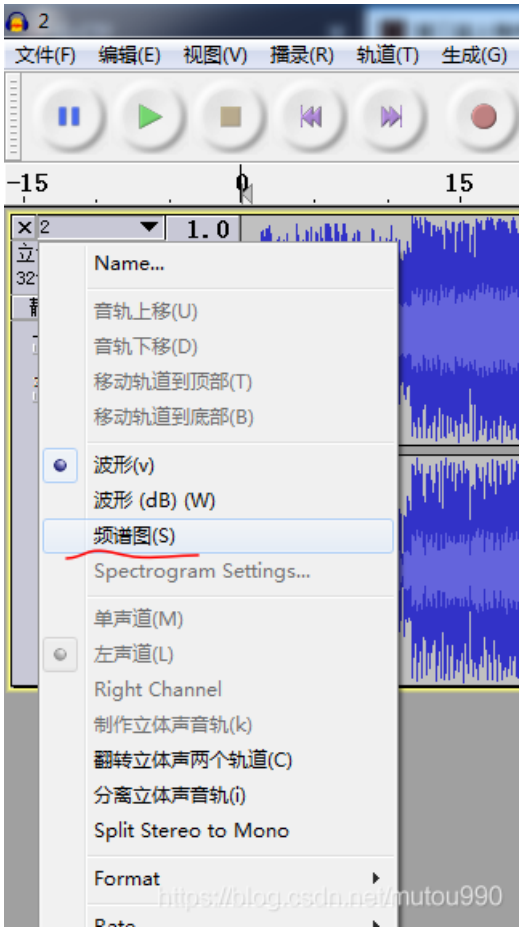
然后回到数据包刷新一下就可以看到揭秘之后的数据了。因为TLS加密的是http协议，所以解密之后直接过滤http协议就可以了。

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不难知道要得到真正的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