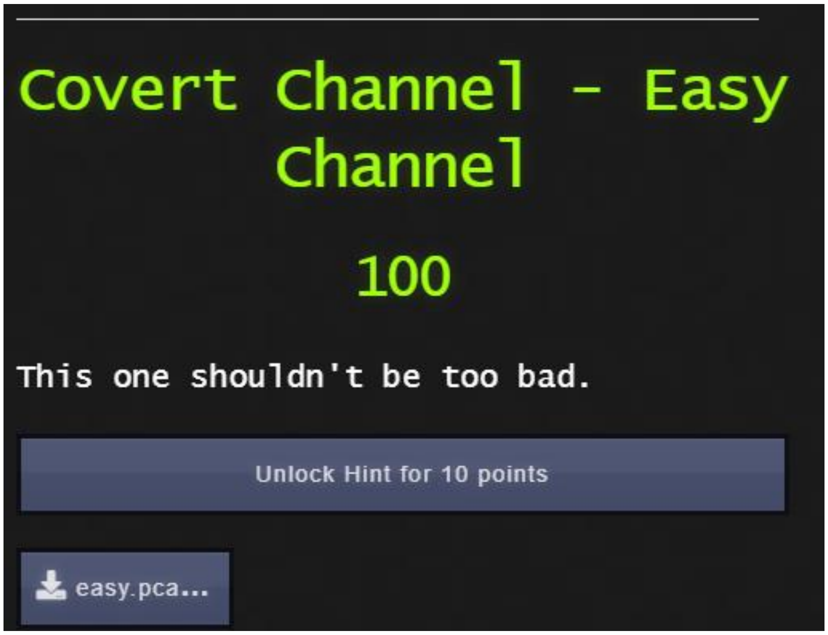


Covert Channel - Easy Channel

100

This one shouldn't be too bad.

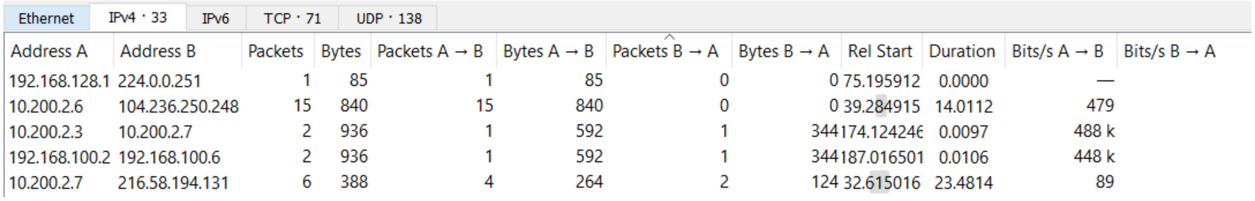
This one with the right knowledge on what to look for is quite easy to spot.

On the surface this can take some digging but we will show how to find he 15 packets that create the flag.

I am not going to dig into all the rabbit holes I went down first, before I stumbled across this odd item that made it stick out like a sore thumb. (looking at protocol hierarchy, DNS tunneling, etc.)

The key to solving this challenge is to look at Conversations, and it is not the most or least conversations, it was a one-way conversation that had traffic going in one direction.

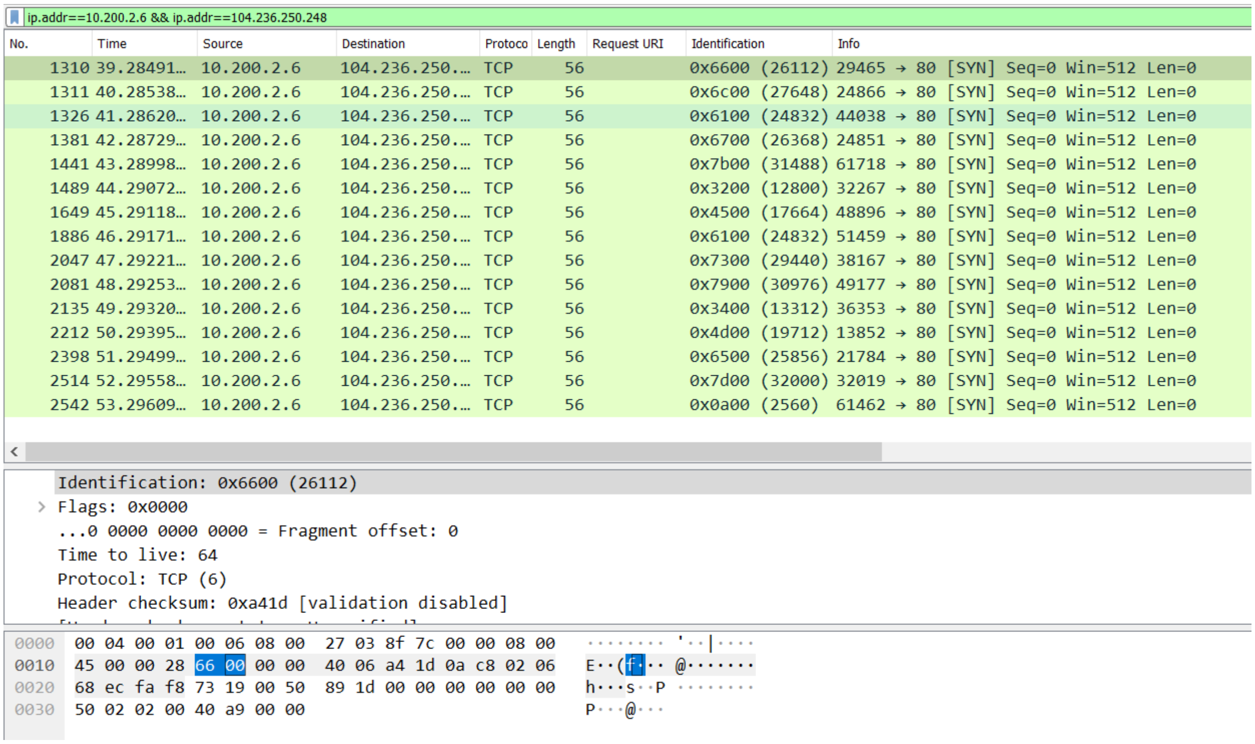
Filter on Packets B -> A and this is really easy to spot some odd stuff going on here.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.128.1	224.0.0.251	1	85	1	85	0	0	75.195912	0.0000	—	
10.200.2.6	104.236.250.248	15	840	15	840	0	0	39.284915	14.0112	479	
10.200.2.3	10.200.2.7	2	936	1	592	1	344	174.124246	0.0097	488 k	
192.168.100.2	192.168.100.6	2	936	1	592	1	344	187.016501	0.0106	448 k	
10.200.2.7	216.58.194.131	6	388	4	264	2	124	32.615016	23.4814	89	

Line two above has 15 packets sent and 0 received. Filter on this conversation and our answer is there somewhere.

In the Identification field of the TCP packet is out flag:



ip.addr==10.200.2.6 && ip.addr==104.236.250.248

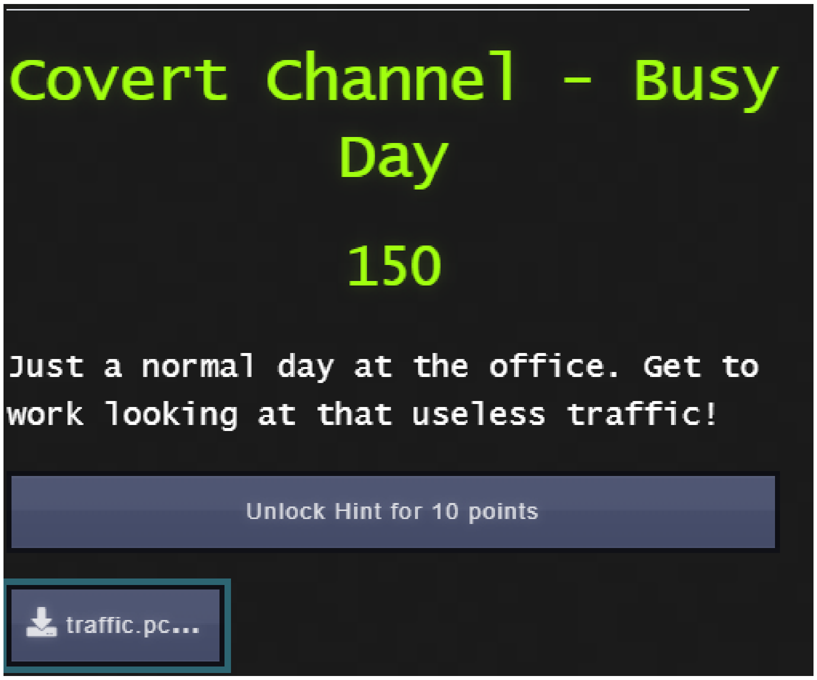
No.	Time	Source	Destination	Protoco	Length	Request URI	Identification	Info
1310	39.28491…	10.200.2.6	104.236.250.…	TCP	56		0x6600 (26112)	29465 → 80 [SYN] Seq=0 Win=512 Len=0
1311	40.28538…	10.200.2.6	104.236.250.…	TCP	56		0x6c00 (27648)	24866 → 80 [SYN] Seq=0 Win=512 Len=0
1326	41.28620…	10.200.2.6	104.236.250.…	TCP	56		0x6100 (24832)	44038 → 80 [SYN] Seq=0 Win=512 Len=0
1381	42.28729…	10.200.2.6	104.236.250.…	TCP	56		0x6700 (26368)	24851 → 80 [SYN] Seq=0 Win=512 Len=0
1441	43.28998…	10.200.2.6	104.236.250.…	TCP	56		0x7b00 (31488)	61718 → 80 [SYN] Seq=0 Win=512 Len=0
1489	44.29072…	10.200.2.6	104.236.250.…	TCP	56		0x3200 (12800)	32267 → 80 [SYN] Seq=0 Win=512 Len=0
1649	45.29118…	10.200.2.6	104.236.250.…	TCP	56		0x4500 (17664)	48896 → 80 [SYN] Seq=0 Win=512 Len=0
1886	46.29171…	10.200.2.6	104.236.250.…	TCP	56		0x6100 (24832)	51459 → 80 [SYN] Seq=0 Win=512 Len=0
2047	47.29221…	10.200.2.6	104.236.250.…	TCP	56		0x7300 (29440)	38167 → 80 [SYN] Seq=0 Win=512 Len=0
2081	48.29253…	10.200.2.6	104.236.250.…	TCP	56		0x7900 (30976)	49177 → 80 [SYN] Seq=0 Win=512 Len=0
2135	49.29320…	10.200.2.6	104.236.250.…	TCP	56		0x3400 (13312)	36353 → 80 [SYN] Seq=0 Win=512 Len=0
2212	50.29395…	10.200.2.6	104.236.250.…	TCP	56		0x4d00 (19712)	13852 → 80 [SYN] Seq=0 Win=512 Len=0
2398	51.29499…	10.200.2.6	104.236.250.…	TCP	56		0x6500 (25856)	21784 → 80 [SYN] Seq=0 Win=512 Len=0
2514	52.29558…	10.200.2.6	104.236.250.…	TCP	56		0x7d00 (32000)	32019 → 80 [SYN] Seq=0 Win=512 Len=0
2542	53.29609…	10.200.2.6	104.236.250.…	TCP	56		0x0a00 (2560)	61462 → 80 [SYN] Seq=0 Win=512 Len=0

```
    Identification: 0x6600 (26112)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xa41d [validation disabled]
```

```
0000  00 04 00 01 00 06 08 00  27 03 8f 7c 00 00 08 00   ········ '··|····
0010  45 00 00 28 66 00 00 00  40 06 a4 1d 0a c8 02 06   E··(f··· @·······
0020  68 ec fa f8 73 19 00 50  89 1d 00 00 00 00 00 00   h···s··P ········
0030  50 02 02 00 40 a9 00 00                            P···@···
```

This displays one character at a time in ASCII on the right-hand side.

Flag: flag{2Easy4Me}



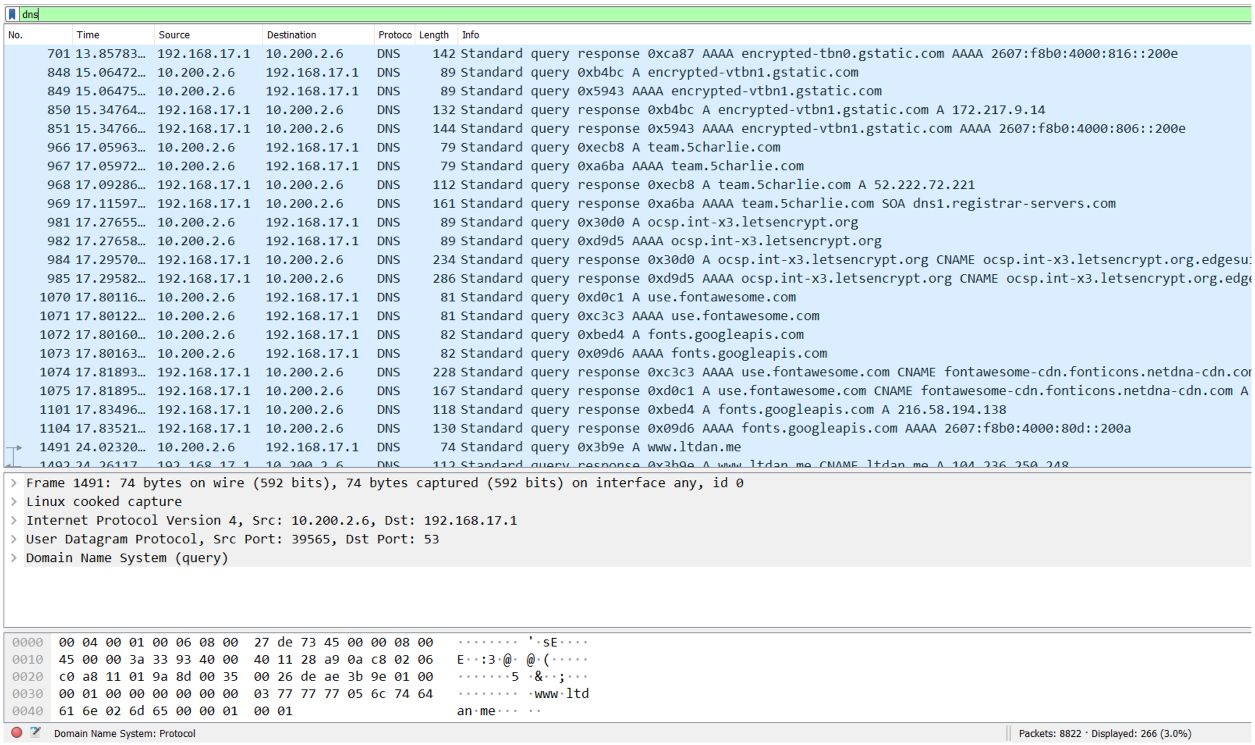
Covert Channel - Busy Day

150

Just a normal day at the office. Get to work looking at that useless traffic!

You can start by looking at the protocol hierarchy and conversations as good practice to start off with on here, but we will see that most of the traffic is encrypted and we will look at that last if we have to look into it.

Let's start off by looking at the low hanging fruit of DNS traffic:



```
dns
No.     Time          Source          Destination     Protoco Length Info
    701 13.85783…     192.168.17.1    10.200.2.6      DNS     142 Standard query response 0xca87 AAAA encrypted-tbn0.gstatic.com AAAA 2607:f8b0:4000:816::200e
    848 15.06472…     10.200.2.6      192.168.17.1    DNS      89 Standard query 0xb4bc A encrypted-vtbn1.gstatic.com
    849 15.06475…     10.200.2.6      192.168.17.1    DNS      89 Standard query 0x5943 AAAA encrypted-vtbn1.gstatic.com
    850 15.34764…     192.168.17.1    10.200.2.6      DNS     132 Standard query response 0xb4bc A encrypted-vtbn1.gstatic.com A 172.217.9.14
    851 15.34766…     192.168.17.1    10.200.2.6      DNS     144 Standard query response 0x5943 AAAA encrypted-vtbn1.gstatic.com AAAA 2607:f8b0:4000:806::200e
    966 17.05963…     10.200.2.6      192.168.17.1    DNS      79 Standard query 0xecb8 A team.5charlie.com
    967 17.05972…     10.200.2.6      192.168.17.1    DNS      79 Standard query 0xa6ba AAAA team.5charlie.com
    968 17.09286…     192.168.17.1    10.200.2.6      DNS     112 Standard query response 0xecb8 A team.5charlie.com A 52.222.72.221
    969 17.11597…     192.168.17.1    10.200.2.6      DNS     161 Standard query response 0xa6ba AAAA team.5charlie.com SOA dns1.registrar-servers.com
    981 17.27655…     10.200.2.6      192.168.17.1    DNS      89 Standard query 0x30d0 A ocsp.int-x3.letsencrypt.org
    982 17.27658…     10.200.2.6      192.168.17.1    DNS      89 Standard query 0xd9d5 AAAA ocsp.int-x3.letsencrypt.org
    984 17.29570…     192.168.17.1    10.200.2.6      DNS     234 Standard query response 0x30d0 A ocsp.int-x3.letsencrypt.org CNAME ocsp.int-x3.letsencrypt.org.edgesu
    985 17.29582…     192.168.17.1    10.200.2.6      DNS     286 Standard query response 0xd9d5 AAAA ocsp.int-x3.letsencrypt.org CNAME ocsp.int-x3.letsencrypt.org.edge
   1070 17.80116…     10.200.2.6      192.168.17.1    DNS      81 Standard query 0xd0c1 A use.fontawesome.com
   1071 17.80122…     10.200.2.6      192.168.17.1    DNS      81 Standard query 0xc3c3 AAAA use.fontawesome.com
   1072 17.80160…     10.200.2.6      192.168.17.1    DNS      82 Standard query 0xbed4 A fonts.googleapis.com
   1073 17.80163…     10.200.2.6      192.168.17.1    DNS      82 Standard query 0x09d6 AAAA fonts.googleapis.com
   1074 17.81893…     192.168.17.1    10.200.2.6      DNS     228 Standard query response 0xc3c3 AAAA use.fontawesome.com CNAME fontawesome-cdn.fonticons.netdna-cdn.cor
   1075 17.81895…     192.168.17.1    10.200.2.6      DNS     167 Standard query response 0xd0c1 A use.fontawesome.com CNAME fontawesome-cdn.fonticons.netdna-cdn.com A
   1101 17.83496…     192.168.17.1    10.200.2.6      DNS     118 Standard query response 0xbed4 A fonts.googleapis.com A 216.58.194.138
   1104 17.83521…     192.168.17.1    10.200.2.6      DNS     130 Standard query response 0x09d6 AAAA fonts.googleapis.com AAAA 2607:f8b0:4000:80d::200a
   1491 24.02320…     10.200.2.6      192.168.17.1    DNS      74 Standard query 0x3b9e A www.ltdan.me
   1492 24.26117…     192.168.17.1    10.200.2.6      DNS     112 Standard query response 0x3b9e A www.ltdan.me CNAME ltdan.me A 104.236.250.248

> Frame 1491: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface any, id 0
> Linux cooked capture
> Internet Protocol Version 4, Src: 10.200.2.6, Dst: 192.168.17.1
> User Datagram Protocol, Src Port: 39565, Dst Port: 53
> Domain Name System (query)

0000  00 04 00 01 00 06 08 00  27 de 73 45 00 00 08 00   ········ '·sE····
0010  45 00 00 3a 33 93 40 00  40 11 28 a9 0a c8 02 06   E··:3·@· @·(·····
0020  c0 a8 11 01 9a 8d 00 35  00 26 de ae 3b 9e 01 00   ·······5 ·&··;···
0030  00 01 00 00 00 00 00 00  03 77 77 77 05 6c 74 64   ········ ·www·ltd
0040  61 6e 02 6d 65 00 00 01  00 01                     an·me··· ··

Domain Name System: Protocol                                   Packets: 8822 · Displayed: 266 (3.0%)
```

This cuts it down to 3% of the total packets.

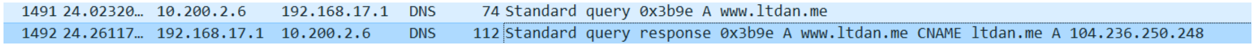
Here we can see the usual stuff that we can ignore like google and such.

Some queries that seem interesting to look at are 5charlie.com, fontawesome.com, ltdan.me, flag, and flag.com

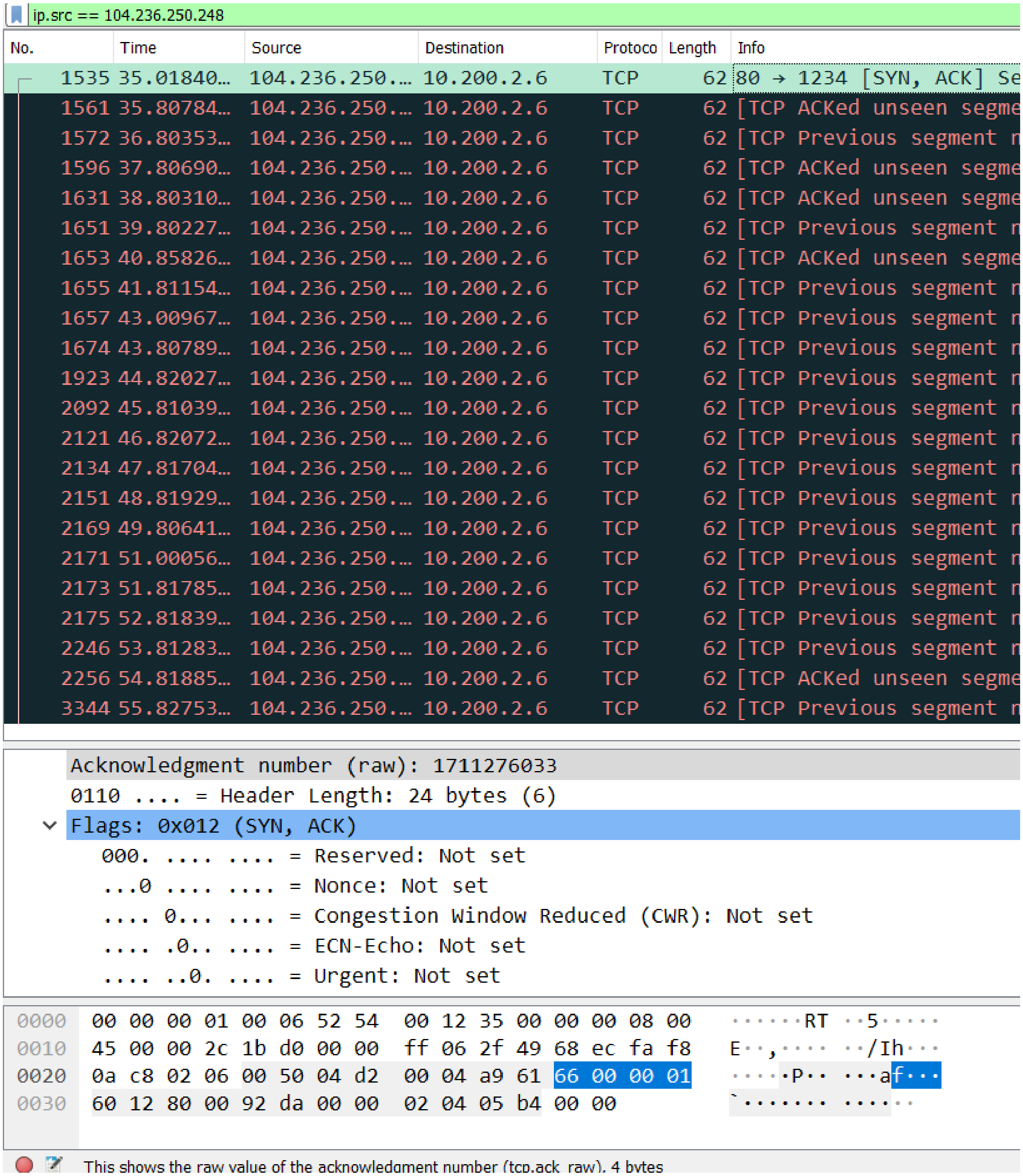
I started down flag and flag.com and quickly realized that they were not of interest, just a couple of pages temporarily moved. This is a Red Herring.

There were tons of packets sent to the 5charlie server, but none were of interest, so that also was a red herring.

The next one of interest was the ltdan.me, and the ip of 104.236.250.248, if we look around this, we see some interesting things happening.



```
1491 24.02320…  10.200.2.6    192.168.17.1  DNS   74 Standard query 0x3b9e A www.ltdan.me
1492 24.26117…  192.168.17.1  10.200.2.6    DNS  112 Standard query response 0x3b9e A www.ltdan.me CNAME ltdan.me A 104.236.250.248
```



ip.src == 104.236.250.248

```
No.   Time        Source          Destination  Protoco Length Info
1535 35.01840…  104.236.250.…  10.200.2.6    TCP       62 80 → 1234 [SYN, ACK] Se
1561 35.80784…  104.236.250.…  10.200.2.6    TCP       62 [TCP ACKed unseen segme
1572 36.80353…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
1596 37.80690…  104.236.250.…  10.200.2.6    TCP       62 [TCP ACKed unseen segme
1631 38.80310…  104.236.250.…  10.200.2.6    TCP       62 [TCP ACKed unseen segme
1651 39.80227…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
1653 40.85826…  104.236.250.…  10.200.2.6    TCP       62 [TCP ACKed unseen segme
1655 41.81154…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
1657 43.00967…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
1674 43.80789…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
1923 44.82027…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2092 45.81039…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2121 46.82072…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2134 47.81704…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2151 48.81929…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2169 49.80641…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2171 51.00056…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2173 51.81785…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2175 52.81839…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2246 53.81283…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
2256 54.81885…  104.236.250.…  10.200.2.6    TCP       62 [TCP ACKed unseen segme
3344 55.82753…  104.236.250.…  10.200.2.6    TCP       62 [TCP Previous segment n
```

```
    Acknowledgment number (raw): 1711276033
    0110 .... = Header Length: 24 bytes (6)
  v Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
```

```
0000  00 00 00 01 00 06 52 54  00 12 35 00 00 00 08 00   ······RT ··5·····
0010  45 00 00 2c 1b d0 00 00  ff 06 2f 49 68 ec fa f8   E··,···· ··/Ih···
0020  0a c8 02 06 00 50 04 d2  00 04 a9 61 66 00 00 01   ·····P·· ···af···
0030  60 12 80 00 92 da 00 00  02 04 05 b4 00 00         `······· ····
```

This shows the raw value of the acknowledgment number (tcp.ack_raw), 4 bytes

Flag is in the sequence numbers on the ip.dst or acknowledgement number for ip.src.

Flag: flag{BouncinPackets!}