Leaky_Stream

Description

In the middle of our conversation, some packets went amiss. We managed to resend a few but they were slightly altered.
Help me reconstruct the message and I'll reward you with something useful ;)

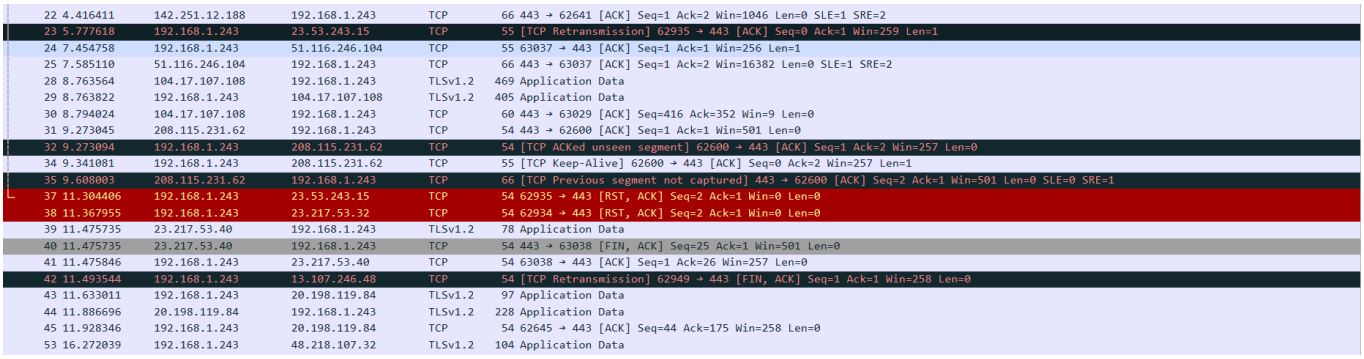
Category

#forensics

Solution

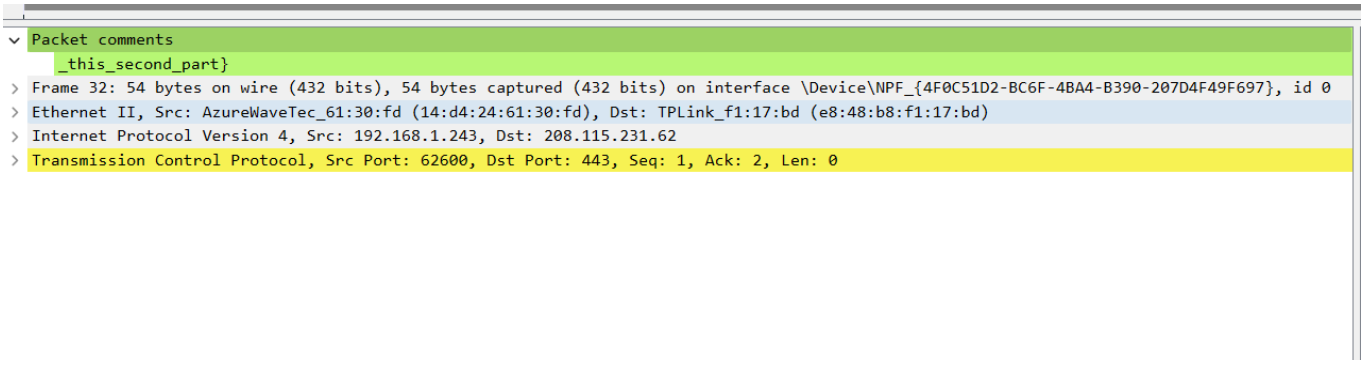
We have a pcap file. Since it was a conversation, packets went missing and resend ability. We can be almost certain that we are dealing with TCP.

It is kinda laboursome, we have to check every resent packet, colored in black



22	4.416411	142.251.12.188	192.168.1.243	TCP	66 443 → 62641 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
23	5.777618	192.168.1.243	23.53.243.15	TCP	55 [TCP Retransmission] 62935 → 443 [ACK] Seq=0 Ack=1 Win=259 Len=1
24	7.454758	192.168.1.243	51.116.246.104	TCP	55 63037 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1
25	7.585110	51.116.246.104	192.168.1.243	TCP	66 443 → 63037 [ACK] Seq=1 Ack=2 Win=16382 Len=0 SLE=1 SRE=2
28	8.763564	104.17.107.108	192.168.1.243	TLSv1.2	469 Application Data
29	8.763822	192.168.1.243	104.17.107.108	TLSv1.2	405 Application Data
30	8.794024	104.17.107.108	192.168.1.243	TCP	60 443 → 63029 [ACK] Seq=416 Ack=352 Win=9 Len=0
31	9.273045	208.115.231.62	192.168.1.243	TCP	54 443 → 62600 [ACK] Seq=1 Ack=1 Win=501 Len=0
32	9.273094	192.168.1.243	208.115.231.62	TCP	54 [TCP ACKed unseen segment] 62600 → 443 [ACK] Seq=1 Ack=2 Win=257 Len=0
34	9.341081	192.168.1.243	208.115.231.62	TCP	55 [TCP Keep-Alive] 62600 → 443 [ACK] Seq=0 Ack=2 Win=257 Len=1
35	9.608003	208.115.231.62	192.168.1.243	TCP	66 [TCP Previous segment not captured] 443 → 62600 [ACK] Seq=2 Ack=1 Win=501 Len=0 SLE=0 SRE=1
37	11.304406	192.168.1.243	23.53.243.15	TCP	54 62935 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
38	11.367955	192.168.1.243	23.217.53.32	TCP	54 62934 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
39	11.475735	23.217.53.40	192.168.1.243	TLSv1.2	78 Application Data
40	11.475735	23.217.53.40	192.168.1.243	TCP	54 443 → 63038 [FIN, ACK] Seq=25 Ack=1 Win=501 Len=0
41	11.475846	192.168.1.243	23.217.53.40	TCP	54 63038 → 443 [ACK] Seq=1 Ack=26 Win=257 Len=0
42	11.493544	192.168.1.243	13.107.246.48	TCP	54 [TCP Retransmission] 62949 → 443 [FIN, ACK] Seq=1 Ack=1 Win=258 Len=0
43	11.633011	192.168.1.243	20.198.119.84	TLSv1.2	97 Application Data
44	11.886696	20.198.119.84	192.168.1.243	TLSv1.2	228 Application Data
45	11.928346	192.168.1.243	20.198.119.84	TCP	54 62645 → 443 [ACK] Seq=44 Ack=175 Win=258 Len=0
53	16.272039	192.168.1.243	48.218.107.32	TLSv1.2	104 Application Data

We found a frame that has a comment



```
Packet comments
    _this_second_part}
Frame 32: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{4F0C51D2-BC6F-4BA4-B390-207D4F49F697}, id 0
Ethernet II, Src: AzureWaveTec_61:30:fd (14:d4:24:61:30:fd), Dst: TPLink_f1:17:bd (e8:48:b8:f1:17:bd)
Internet Protocol Version 4, Src: 192.168.1.243, Dst: 208.115.231.62
Transmission Control Protocol, Src Port: 62600, Dst Port: 443, Seq: 1, Ack: 2, Len: 0
```

Therefore, we can expect that, the other packet also has a commet