

流量包很小，显然考察的是 IEC 60870-5-104 电力规约协议，该协议的报文解析可以参考 <https://blog.csdn.net/ZhangYu971014/article/details/135889376>，我们主要关注 I 格式报文，因为数据通常以 I 为载体传输，flag 很大可能隐藏在里面。

我们在 wireshark 中关注协议一列带有 ASDU（应用服务数据单元）的流量，这意味着客户端可能发送了一个新的命令。

Frame 65: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPFLP\_Loopback, id 0  
 Null/loopback  
 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 Transmission Control Protocol, Src Port: 61597, Dst Port: 2404, Seq: 145, Ack: 97, Len: 16  
 IEC 60870-5-104: < I (5,18)  
 - IEC 60870-5-104 ASDU-1 C\_IC\_NA\_1 Act IOA=0 'interrogation command'  
 TypeId: C\_IC\_NA\_1 (100)  
 0... = No: False  
 .000 0001 NumIx: 1  
 ..00 0110 = CauseTx: Act (6)  
 .0... .... = Negative: False  
 0... .... = Test: False  
 OA: 2

注意到 65 号流量处发送了一个总召命令（类型标识符为 100），然后下面接着有连续多个 32 位位串信息，怀疑这里可能传输了重要信息，根据报文格式可以将内容提取出来（每个位串信息里只包含了 4 个字节的内容，夹在上一个位串信息的 IOA 和下一个位串信息的 START 标识符中间）。

Source IP	Destination IP	Protocol	Source Port	Destination Port	Sequence Number	Acknowledgment Number	Length	Data
67.264.877144	127.0.0.1	IEC 60870-5 ASDU	63	251.376417	93 <- I (18,6)	> I (19,6) ASDU-4 M_NB_1 Spont	IOA+1336	-> I (20,6) ASDU-4 M_NB_1 Spont IOA+1337
67.264.877144	127.0.0.1	IEC 60870-5 ASDU	64	251.376470	44 61597 > 2404 [ACK] Seq=145 Len=0	44 2404 > 61597 [ACK] Seq=97 Ack=145 Win=255 Len=0		
67.264.877144	127.0.0.1	IEC 60870-5 ASDU	65	264.865899	50 <- I (5,18) ASDU-1 C_IC_NA_1 Act IOA=0	44 2404 > 61597 [ACK] Seq=97 Ack=145 Win=255 Len=0		
67.264.865986	127.0.0.1	TCP	66	264.865986	44 2404 > 61597 [ACK] Seq=97 Ack=145 Win=255 Len=0	44 2404 > 61597 [ACK] Seq=97 Ack=145 Win=255 Len=0		
67.264.877144	127.0.0.1	IEC 60870-5 ASDU	67	264.877144	93 >- I (18,6)   -> I (19,6) ASDU=47 M_ME_NB_1 Spont IOA=0	44 2404 > 61597 [ACK] Seq=97 Ack=145 Win=255 Len=0		
68.264.977226	127.0.0.1	TCP	68	264.977226	234 -> I (21,6) ASDU=47 M_BO_NA_1 Spont IOA=1338   -> I (22,6)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
69.264.977168	127.0.0.1	IEC 60870-5 ASDU	69	264.977168	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
70.264.977218	127.0.0.1	TCP	70	264.977218	234 -> I (21,6) ASDU=47 M_BO_NA_1 Spont IOA=1338   -> I (22,6)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
71.264.979133	127.0.0.1	IEC 60870-5-104	71	264.979133	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
72.264.979180	127.0.0.1	TCP	72	264.979180	50 <- S (26)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
73.265.076959	127.0.0.1	IEC 60870-5 ASDU	73	265.076959	131 -> I (31,6) ASDU=47 M_BO_NA_1 Spont IOA=1348   -> I (32,6)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
74.265.077038	127.0.0.1	TCP	74	265.077038	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
75.265.080679	127.0.0.1	IEC 60870-5-104	75	265.080679	50 <- S (34)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
76.265.080757	127.0.0.1	TCP	76	265.080757	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
80.274.693581	127.0.0.1	IEC 60870-5-104	80	274.693581	50 >- U (TESTFR con)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
82.274.694368	127.0.0.1	TCP	82	274.694368	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
83.294.777081	127.0.0.1	IEC 60870-5-104	83	294.777081	50 >- U (TESTFR act)	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		
84.294.777138	127.0.0.1	TCP	84	294.777138	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0	44 61597 > 2404 [ACK] Seq=161 Ack=146 Win=254 Len=0		

得到 ZmxhZ3s4NmQ4ZTg3Yi1hYTbjLTQ5MTktYmU1Mi01ZjI5NzE2NmQ3ZjB9，base64 解码得到 flag{86d8e87b-aa0c-4919-be52-5f297166d7f0}