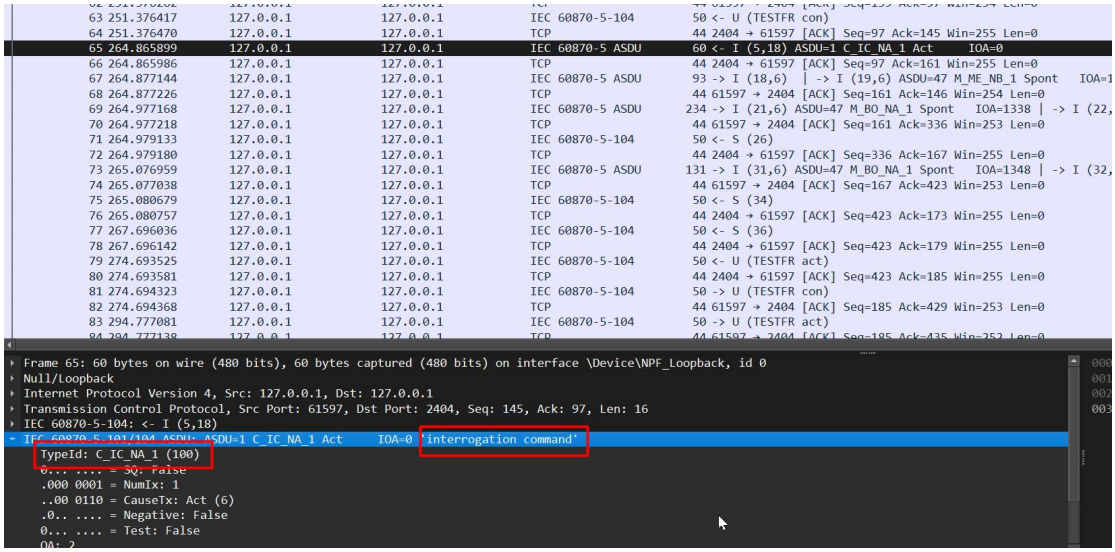
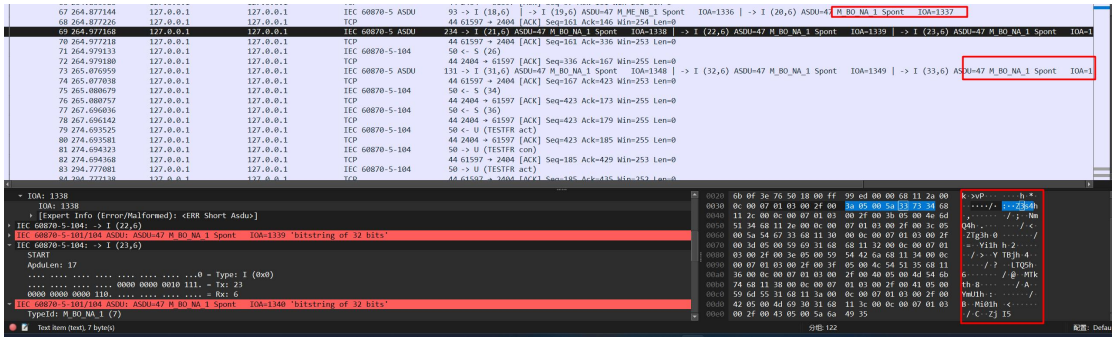
流量包很小，显然考察的是 IEC 60870-5-104 电力规约协议，该协议的报文解析可以参考 https://blog.csdn.net/ZhangYu971014/article/details/135889376，我们主要关注 I 格式报文，因为数据通常以 I 为载体传输，flag 很大可能隐藏在里面。

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。



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）。



得到 ZmxhZ3s4NmQ4ZTg3Yi1hYTBjLTQ5MTktYmU1Mi01ZjI5NzE2NmQ3ZjB9，base64 解码得到 flag{86d8e87b-aa0c-4919-be52-5f297166d7f0}