使用OmniPeek抓取终端关联到AP（开放认证SSID） 过程配置案例

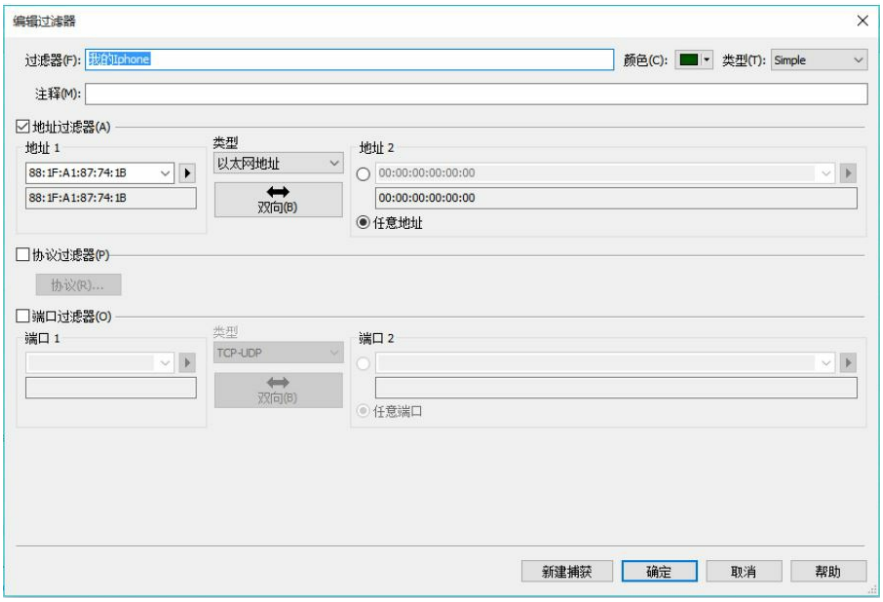
SSID wlan优化 陈少华 2017-07-31 发表

借助OmniPeek 抓取终端关联到AP的过程，通过对无线报文的分析了解无线终端关联过程，及无线网络的运行状况对处理分析无线关联问题，例如：终端关联失败、无线终端丢包等起到极大帮助作用。

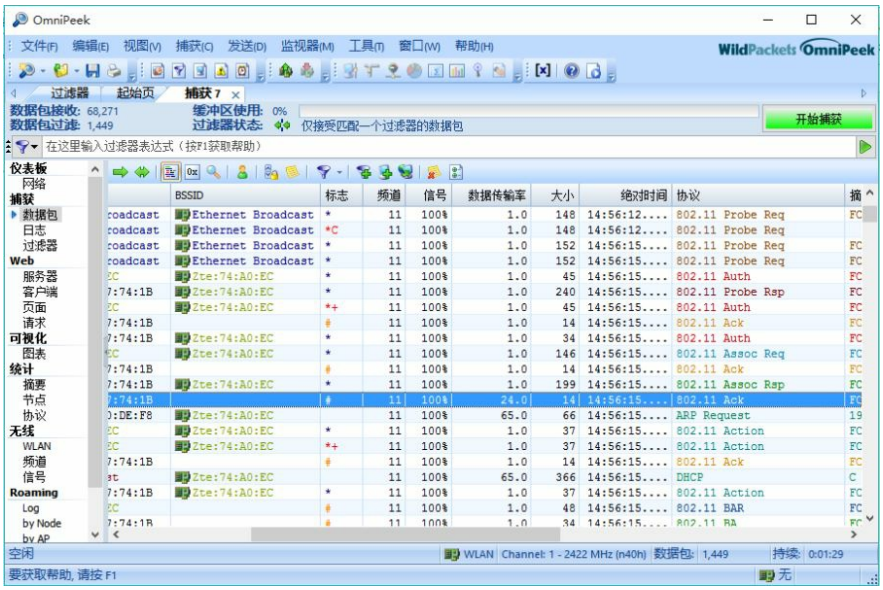
开放认证的SSID

连接到BSS需要两个步骤，即认证和关联。下面我们通过抓包来逐步认识一下这一过程。

由于一开始我们并不知道关联过程中有哪些类型的报文参与其中，所以我们将过滤器的筛选粒度设置的大一些，抓取终端发送和接收的所有报文。

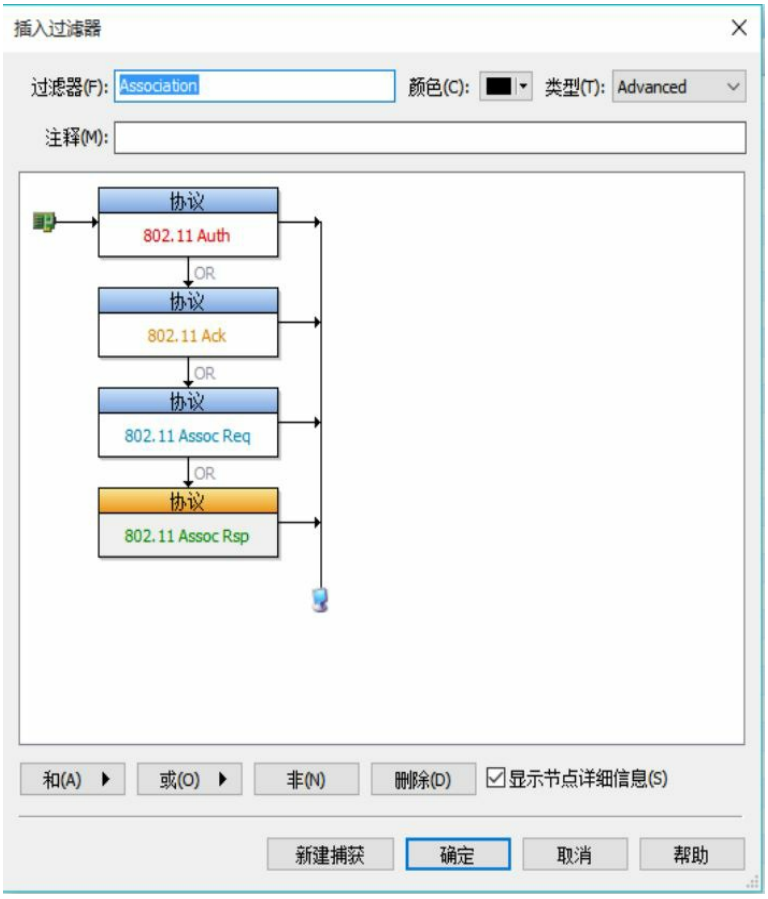


开始捕获，然后关联上CMCC-WEB。

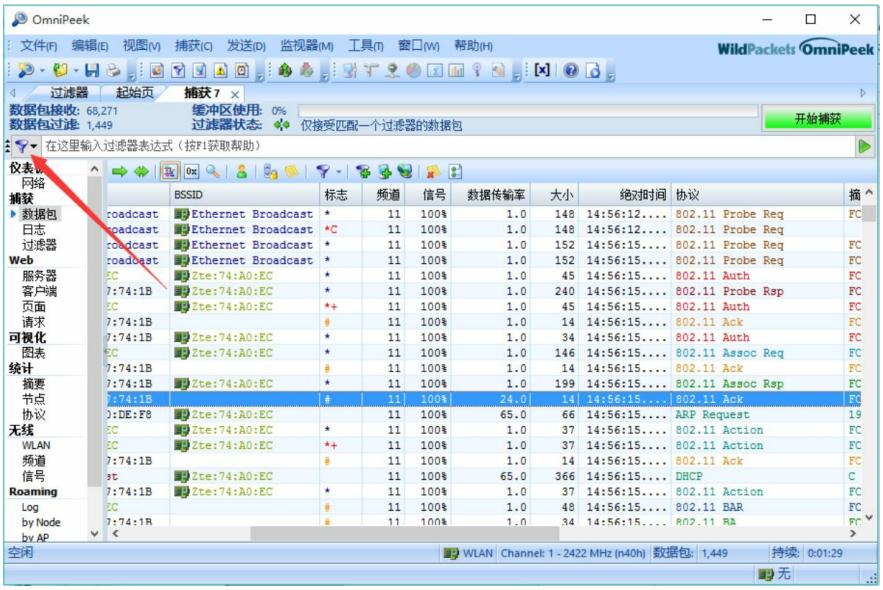


可以看到从第一个802.11 Auth帧开始，到第一个ARP Req结束，共有802.11 Ack、802.11 Auth、802.11 Assoc Req、和802.11 Assoc Rsp 4种类型的帧参与。于是我们剔除其他帧，排除干扰。

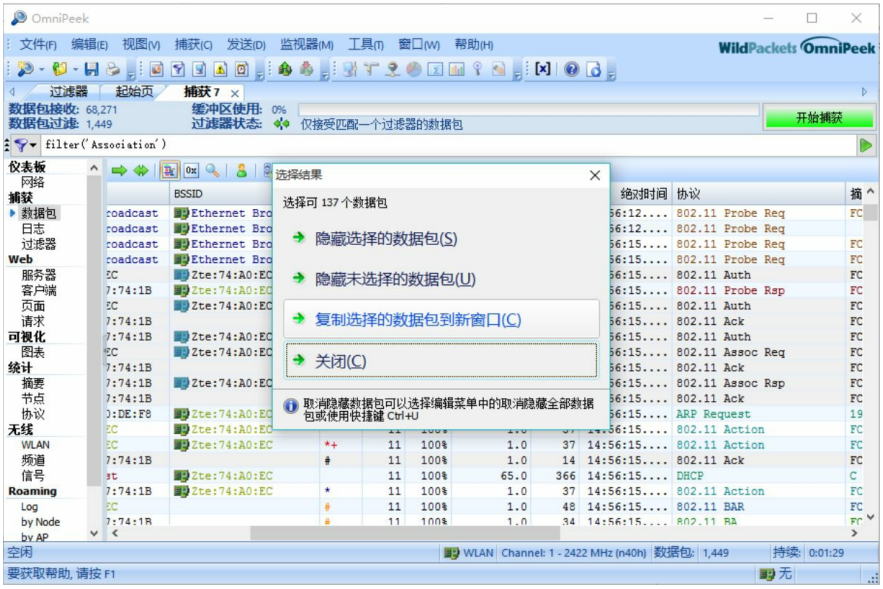
新建过滤器，在高级模式下选择上面的协议。

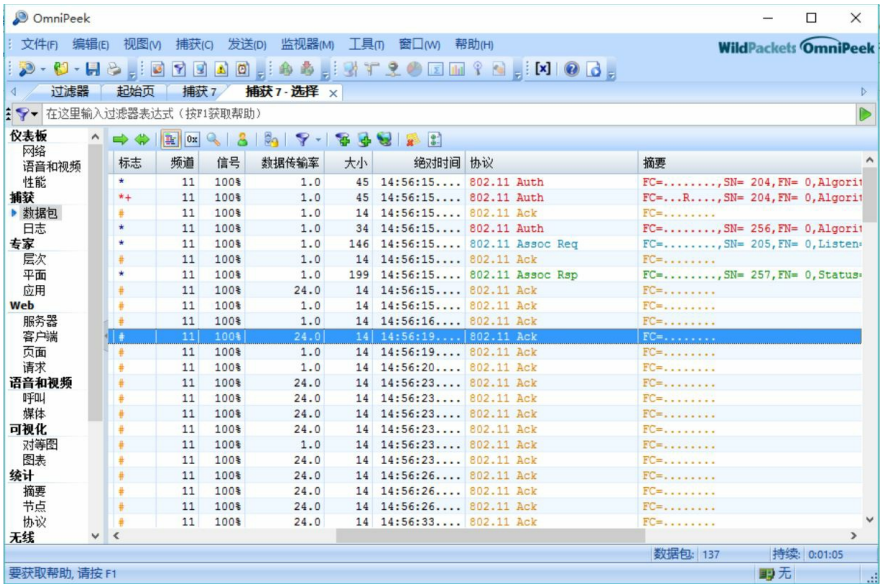


在捕获窗口点击左上角的筛选按钮，插入我们刚刚新建的过滤器。



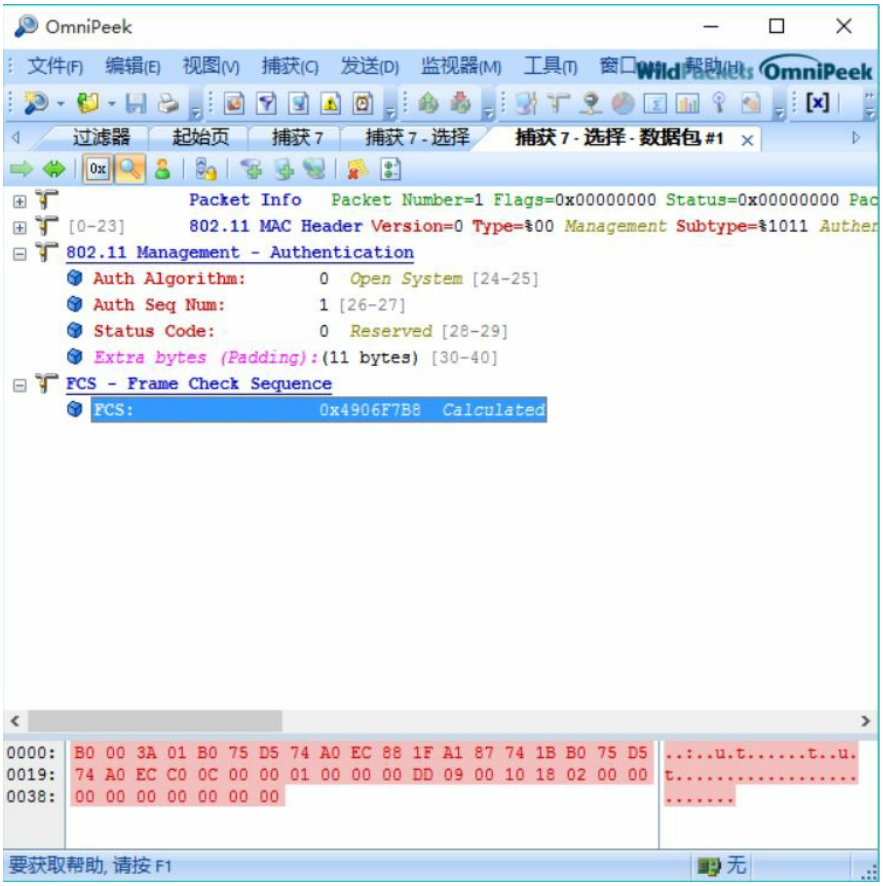
复制选择的报文到新窗口



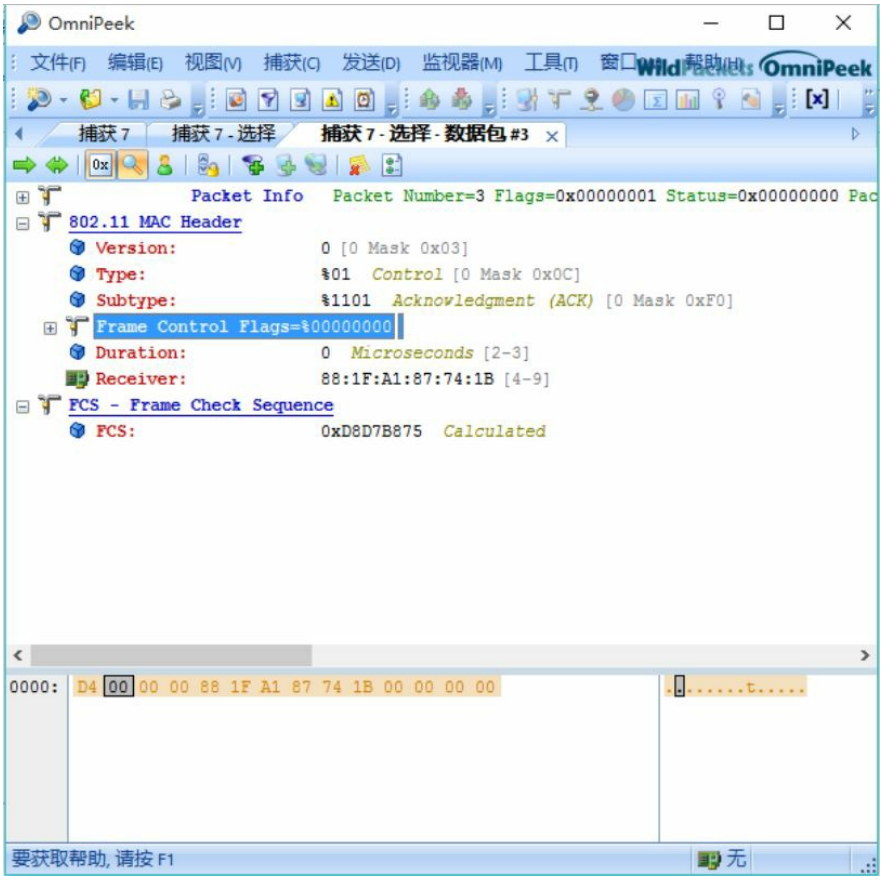


可以看到，除了我们需要的报文之外，还有很多ACK混了进来。这是因为AP在每收到终端的一条数据之后都会返回一条ACK。

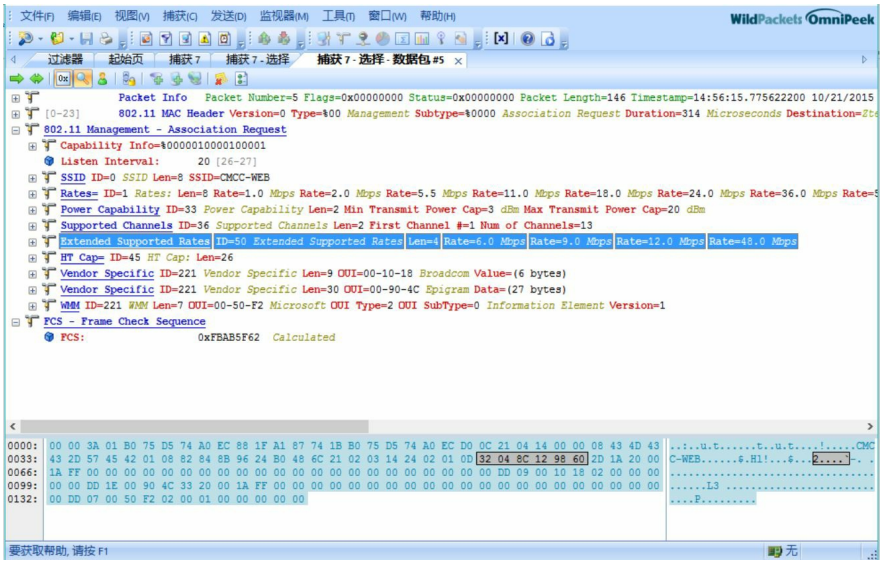
点开802.11 Auth报文，可以看到由于这个SSID是未加密的，所以这个报文内容非常简单。



802.11 Ack的内容也非常简单，只有MAC子层报头而已。

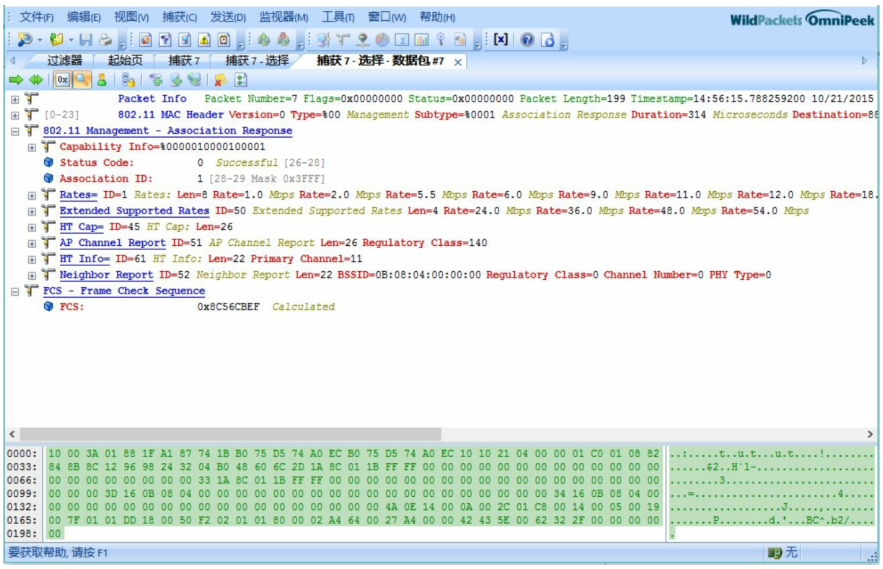


802.11 Assoc Req终于有内容了，仔细看看是不是跟Beacon帧的内容类似。



注意这是终端发送给AP的，终端在哪里知道的这些信息呢？方法有两种：主动扫描和被动扫描。

802.11 Assoc Rsp，相当于精简了的802.11 Probe Rsp



通过以上一系列交互，终端终于成功关联上了AP。