**Wireshark解析插件使用说明**

**步骤一 lua文件配置**

**Lua文件SVN地址:**

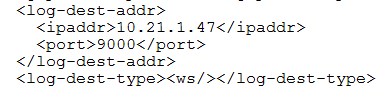
**svn://10.21.1.188/lte\_henb/tool/L1API\_msg\_dissector**

将lua文件放在wireshark根目录下，并在根目录下的init.lua文件后添加相应的语句，

dofile("XX.lua")

**步骤二 端口配置**

Lua解析脚本中的类似udp\_encap\_table:add(9000,p\_logprot)语句是用来设置解析时使用的udp端口，S1,RRC,LOG均使用了9000端口。然后在协议里面设置wireshark所在主机ip和接收端口，S1和LOG的端口在cfg.xer中设置，



RRC在rrc\_tx.c中设置



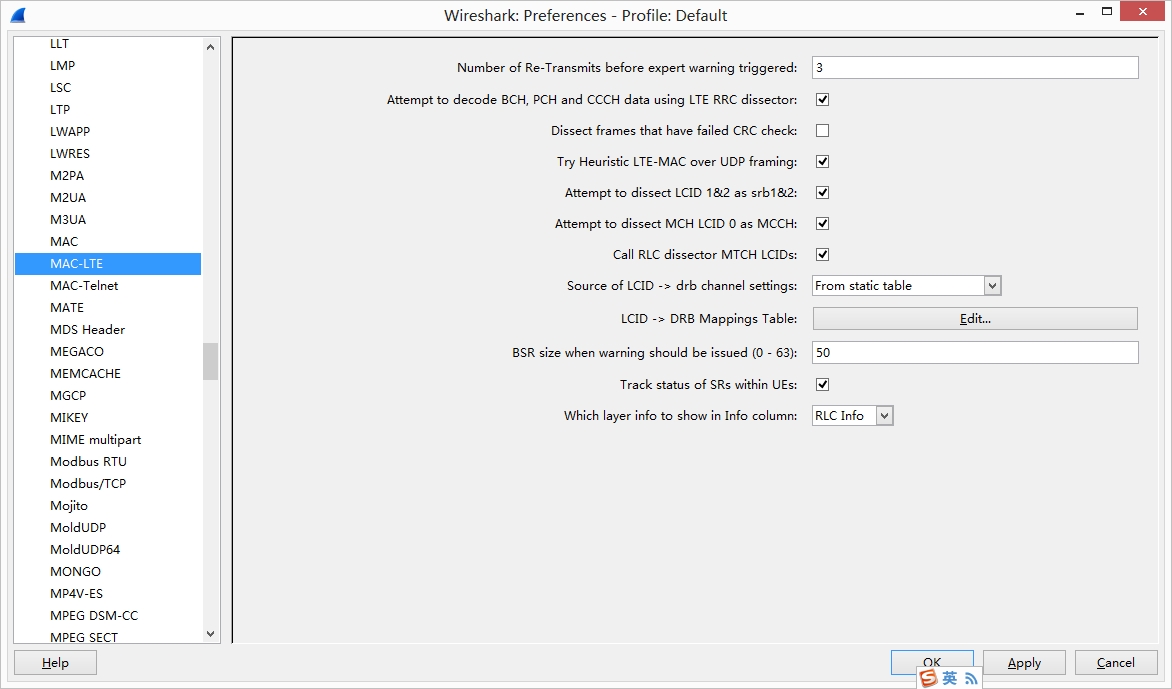
L1api在fs\_l1api\_encode.c中设置



MAC-LTE在mac\_lte\_logger.c中设置

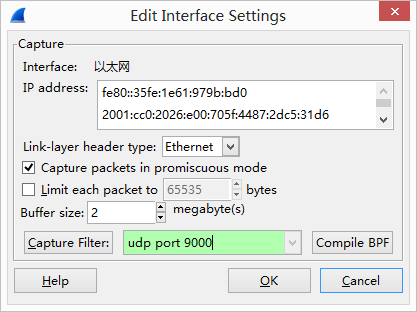


注意在使用MAC-LTE的时候，需要在wireshark->edit->preferences中打开MAC-LTE在udp协议的启发式解析功能，如下图示



另外当udp包大于1500的时候，IP协议会分段，导致MAC-LTE包不能解析，

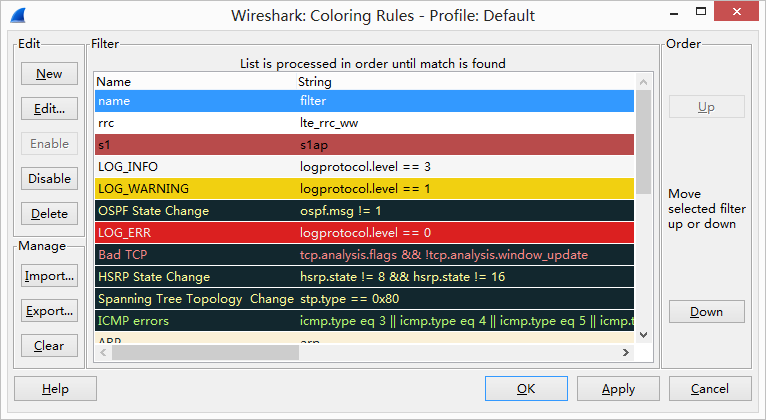
**步骤三抓取**

打开wireshark，

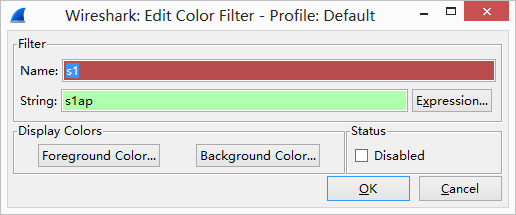
设置过滤的协议和端口后，Start，这时候运行协议栈，wireshark就可以解析收到的包了

**步骤四颜色配置**

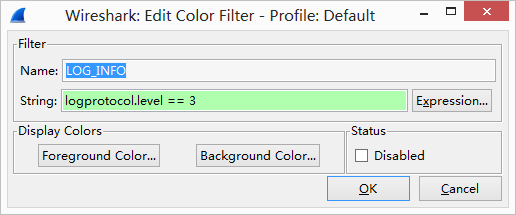
Wireshark提供了逻辑表达式设置相应的包的颜色，在View -> coloring rules,



然后new一个新的颜色规则，分别填上名字和相应的表达式，比如S1和LOG



在LOG解析模块中，可以用logprotocol.level == 1, logprotocol.level == 2,logprotocol.level == 3,logprotocol.level == 4来区分不同的等级，设置不同的颜色

  
另外这些颜色规则，是从上到下递减优先级，可以调整颜色规则的顺序，如果颜色冲突，将采用高优先级的