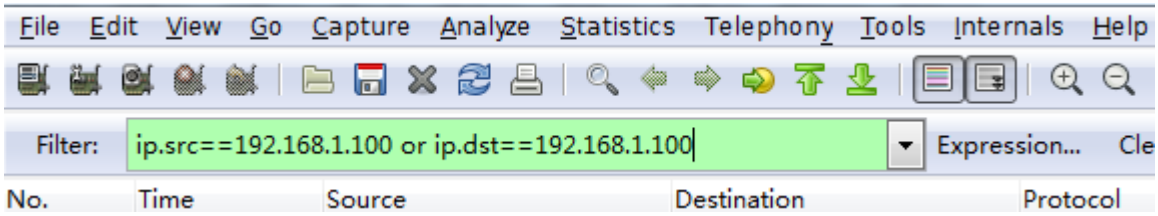
用 wireshark 过滤特定主机数据包

工作中经常用到 wireshark，写一些如下的表达式进行过滤和特定主机的通信：

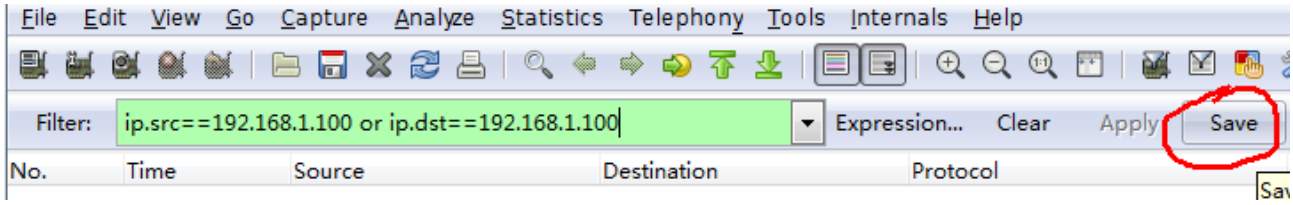
ip.src==192.168.1.100 or ip.dst==192.168.1.100

如图所示：

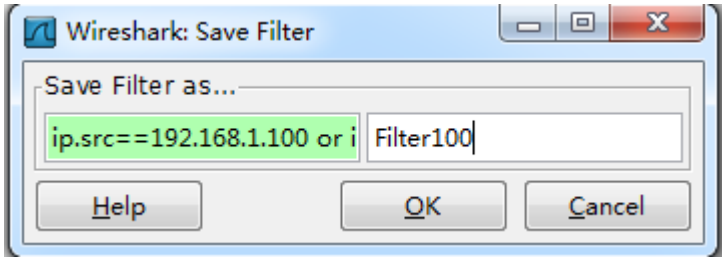


由于 wireshark 中的 Filter 框的下拉列表只有两个历史记录（这个我暂时没有找到配置的地方……），如果涉及的主机比较多的话，需要每次输入过滤器中的 ip（或者更改），感觉比较麻烦。由于这段时间经常用，发现一个小技巧，这里写出来分享给大家，不足之处欢迎指出。

我们可以看到，在 Filter 框的右侧有个 Save 按钮：

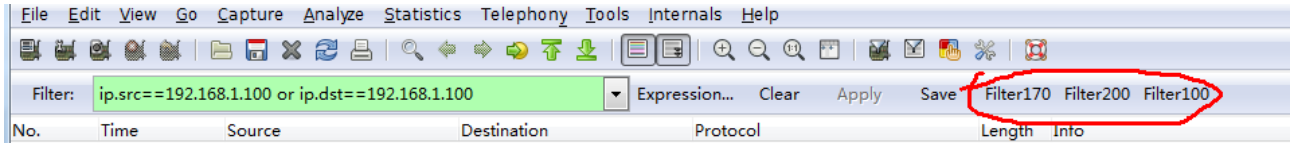


点击 Save 按钮，弹出如下对话框（我填了“Filer100”）：



点击 OK 后，发现在右侧出现了个 Filter100 的按钮，把 Filter 框中的内容清除掉，然后点击 Filter100 这个按钮，Filter 框会自动填充之前的表达式，并对数据包进行过滤。

感觉用起来比较方便，如果多设置几个，在抓包过程中的过滤就方便多了：



如果表达式不再需要或者需要管理的话，可以通过“Edit”==》 “Preferences”==》“Filter Expressions”进行操作。