

## 4.5 过滤器

过滤器允许你找出所希望进行分析的数据包。简单来说，一个过滤器就是定义了一定的条件，用来包含或者排除满足自定义条件的数据包的表达式。如果你不希望看到一些数据包，则可以写一个过滤器来屏蔽它们；如果你希望只看到某些数据包，则可以写一个过滤器来只显示出这些数据包。

Wireshark 主要提供两种主要的过滤器。

- 捕获过滤器：当进行数据包捕获时，只有那些满足给定的包含/排除表达式的数据包会被捕获。
- 显示过滤器：该过滤器根据指定的表达式用于一个已捕获的数据包集合，它将隐藏不想显示的数据包，或者只显示那些需要的数据包。

我们先看一下捕获过滤器。