## 4.2.1 保存和导出捕获文件

如果想要找到符合特定条件的数据包，那么可以按 Ctrl-F 组合键打开 Find Packet 条形框，如图 4-4 方框内所示。这个条形框应该在过滤框和 列表窗口之间。

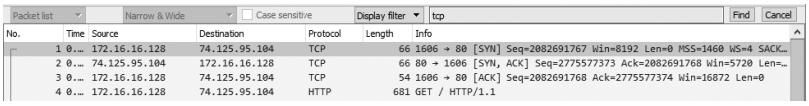


图 4-4　在 Wireshark 中根据条件查找数据包——在这个案例中，只有数据包符合 达式 TCP 才会被显示出来

这个对话框为查找数据包提供了 3 个选项。

- Display filter 选项允许你通过输入表达式进行筛选，并只找出那些满足该 达式的数据包，就像在图 4-4 中所使用的那样。
- Hex Value 选项使用你所输入的十六进制数，对数据包进行搜索。
- String 选项使用你所输入的字符串，对数据包进行搜索。你可以在搜索面 上设置是否区分大小写和其他的格式。

表 4-1 给出了上述几种搜索类型的例子。

**表 4-1　用来查找数据包的搜索类型**

| 搜索类型 | 例子 |
| --- | --- |
| Display Filter | not ip |
| | ip.addr==192.168.0.1 |
| | arp |
| Hex value | 00:ff |
| | ff:ff |

| 搜索类型 | 例子 |
| --- | --- |
| | 00:AB:B1:f0 |
| String | Workstation1 |
| | User8 |
| | Domain |

在确定选项并在文本框中输入搜索关键词之后，单击 Find，就会找到满足该关键词的第一个数据包。如果想要找到下一个匹配的数据包，则按 Ctrl-N 组合键；想要找到前一个，则按 Ctrl-B 组合键。