5.8 专家信息

Wireshark 中每个协议的解析器都有一些专家信息，可以提醒你该协议的数据包中的特定状态。这些状态可以分为 4 类。

对话：关于通信的基本信息。

注意：正常通信中的异常数据包。

警告：非正常通信中的异常数据包。

错误：数据包中的错误，或者解析器解析时的错误。

举例来说，打开 download-slow.pcapng 这个文件，然后单击 Analyze，并选择 Expert Info Composite，便可以打开这个捕获文件的专家信息窗口。然后反选 Group by summary 来依据严重性排序输出（见图 5-23）。

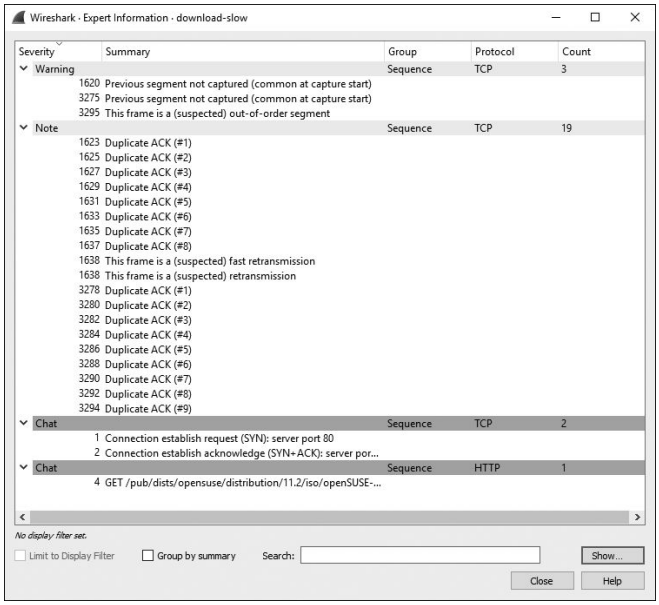

图 5-23　专家信息窗口给出了协议解析器中内置专家系统的信息

我们应该注意到，这个窗口中对于每种类型的信息都有一个选项卡，在这个例子中没有错误消息，但有 3 个警告、18 个注意以及 3 个对话。

这个捕获文件中的大多数信息都与 TCP 有关，这仅仅是因为专家信息系统传统上常用于该协议。目前，总共为 TCP 配置了 29 种专家信息，并且这些信息在解决捕获文件的问题时非常有用。这些信息可以在满足如下条件

的时候对数据包进行标记（这些消息的意义在我们学习了第 8 章和第 11 章后会更加明了）。

1．对话消息

窗口更新　由接收者发送，用来通知发送者 TCP 接收窗口的大小已被改变。

2．注意消息

TCP 重传输　数据包丢失的结果。当收到重复的 ACK，或者数据包的重传输计时器超时的时候产生。

重复 ACK　当一台主机没有收到下一个期望序列号的数据包时，它会生成其最后收到的一个数据的重复 ACK。

零窗口探查　在一个零窗口包被发送之后，用来监视 TCP 接收窗口的状态（将在第 9 章中介绍）。

保持活动状态 ACK　用来响应保持活动状态数据包。

零窗口探查 ACK　用来响应零窗口探查数据包。

窗口已满　用来通知传输主机接收者的 TCP 接收窗口已满。

3．警告信息

上一段丢失　指明数据包丢失。当数据流中一个期望的序列号被跳过时产生。

收到丢失数据包的 ACK　当一个数据包已经确认丢失但仍收到了其 ACK 数据包时产生。

保持连接状态　当一个连接的保持连接数据包出现时触发。

零窗口　当接收方已经达到 TCP 接收窗口大小时，会发出一个零窗口通知，要求发送方停止传输数据。

乱序　当数据包乱序被接收时，会利用序列号进行检测。

快速重传输　一次重传会在收到一个重复 ACK 的 20ms 内进行。

4．错误消息

没有错误消息

虽然本章中介绍的一些功能看上去只有在偶尔的情况下才会用到，但你可能会发现它们比你想象中要有用得多。你需要熟悉这些窗口和选项，这很重要，因为我会在之后的几个章节中频繁地提到它们。

---

[1] ESPN—娱乐与体育节目电视网，是一个 24 小时专门播放体育节目的美国有线电视联播网。——译者注