4.3.3 时间偏移

有些时候你也许会遇到来自不同源的包数据，它们之间的时间是不同步的。当我们调查从不同地方捕获的相同流量时，这种情况尤为多见。虽然大多数的管理员都会尽可能地保持网络上每一个设备的时间都是同步的，但例外情况时有发生。Wireshark 提供了一项时间偏移的功能，它通过把包的时间戳整体偏移调整，来减轻在分析中可能遇到的麻烦。

要对一个或多个包的时间戳进行偏移调整，只需选择 Edit->Time Shift 或者按下组合键 Ctrl-Shift-T。时间偏移窗口打开后，你就可以设定一个时间区间，来对所有包的时间进行调整，或者针对一个包设置时间戳了。在图 4-9 所示的例子当中，我选择把所有包的时间戳都加上 2min5s。

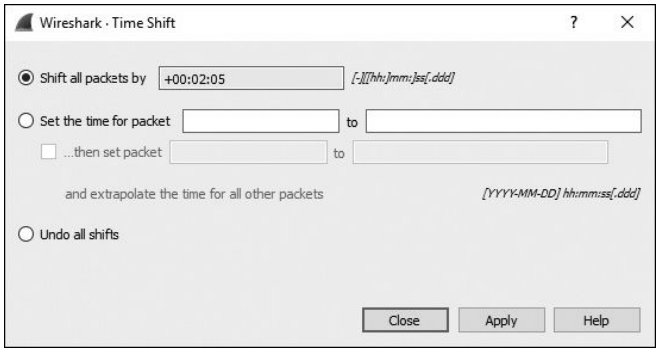

图 4-9　时间偏移窗口