13.3.1 配置 AirPcap

AirPcap（现在是 Riverbed 旗下 CACE Technologies 公司的产品）被设计用来突破 Windows 强加给无线数据包分析的限制。AirPcap 像 U 盘一样小巧，如图 13-5 所示，用于捕获无线流量。AirPcap 使用第 3 章讨论的 WinPcap 驱动和一个特制的客户端配置工具。

图 13-5　AirPcap 的设计非常紧凑，适合与笔记本电脑一同携带

AirPcap 的配置程序很简单，只有一些配置选项。如图 13-6 所示，AirPcap 控制面板提供了以下几个选项。

Interface：你可以在这里选择要捕获的设备。一些高级的分析场景会要求你使用多个 AirPcap 设备，同步嗅探多个信道。

Blink Led：勾选这个复选框会使 AirPcap 设备上的 LED 指示灯闪烁。当存在多个 AirPcap 设备时，这可用来识别正在使用的适配器。

Channel：在这个下拉菜单里，你可以选择希望 AirPcap 监听的信道。

Include 802.11 FCS in Frames：默认情况下，一些系统会抛弃无线数据包的最后 4 个校验和比特。这个被称为帧校验序列（Frame Check Sequence，FCS）的校验和用来确保数据包在传输过程中没有被破坏。除非你有特别的理由，否则请勾选这个复选框（包含 FCS 校验和）。

Capture Type：这里有两个选项——802.11 Only 和 802.11 + Radio。802.11 Only 选项包含标准的 802.11 数据包头。802.11 + Radio 选项包含这个包头以及前端的 radiotap 头部，因而包含额外信息，比如数据率、频率、信号等级和噪声等级。选择 802.11 + Radio 以观察所有可用的数据信息。

FCS Filter：即便你没有选择 Include 802.11 FCS in Frames，这个选项也可以过滤 FCS 认为已经被损坏的数据包。使用 Valid Frames 选项可以只显示 FCS 认为成功接收的那些数据包。

WEP Configuration：这个区域（在 AirPcap Control Panel 的 Keys 选项卡可见）允许你输入所嗅探网络的 WEP 密码。为了能解密 WEP 加密的数据，你需要在这里填入正确的 WEP 密码。WEP 密码将在 13.9 节中讨论。

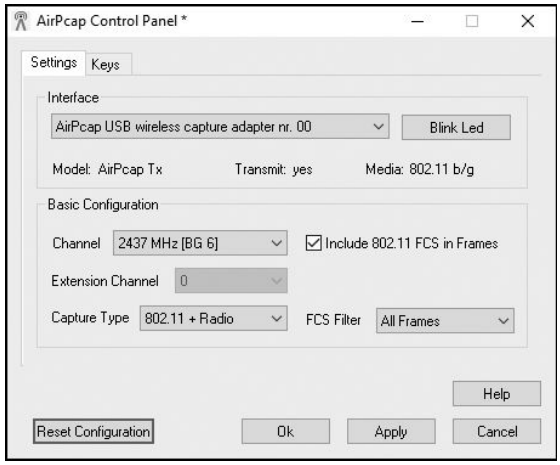

图 13-6　AirPcap 配置程序