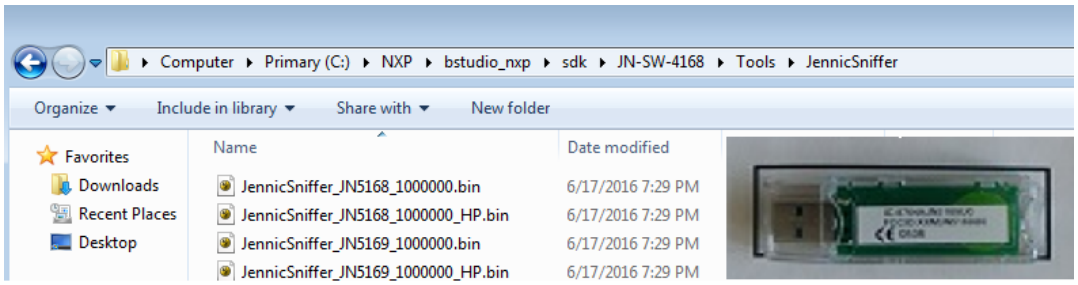
利用 Wireshark 对 ZigBee 及 Thread 进行抓包分析

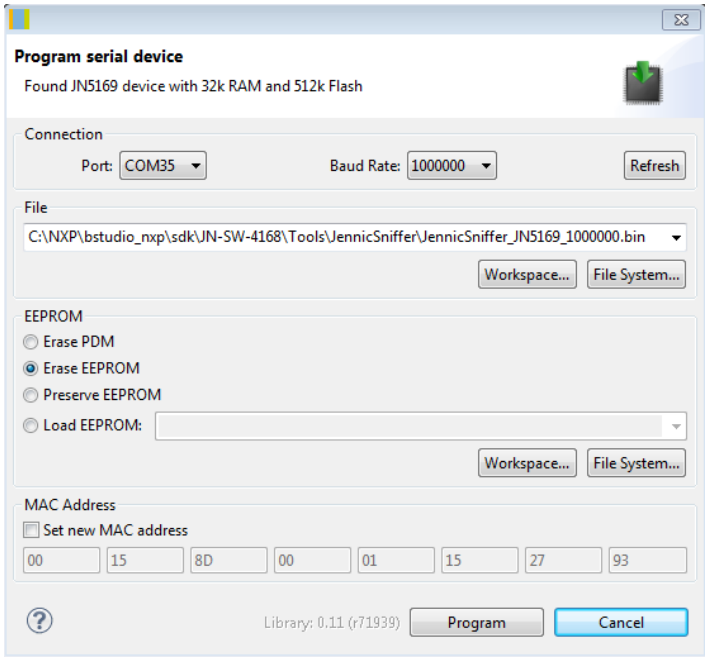
(shaozhong.liang@nxp.com)

无线网络开发人员常常需要抓取空中实际传输的数据包才能分析问题。我们可以使用免费开源的 Wireshark 这款非常著名的网络抓包软件，配合 NXP 的 USB Dongle（JN-5169）实现 IEEE802.15.4 数据抓包和分析 ZigBee/Thread 协议。Wireshark 可以完整解析 ZigBee 协议中 APS、APF、NWK、ZCL、ZDP 等各层协议，支持加密网络的解析。并且可以解析 6LoWPAN 协议中报文压缩协议、RPL 路由协议、ICMPV6、TCP/UDP、NA 等协议。

1. NXP 的 JN5169 USB Dongle

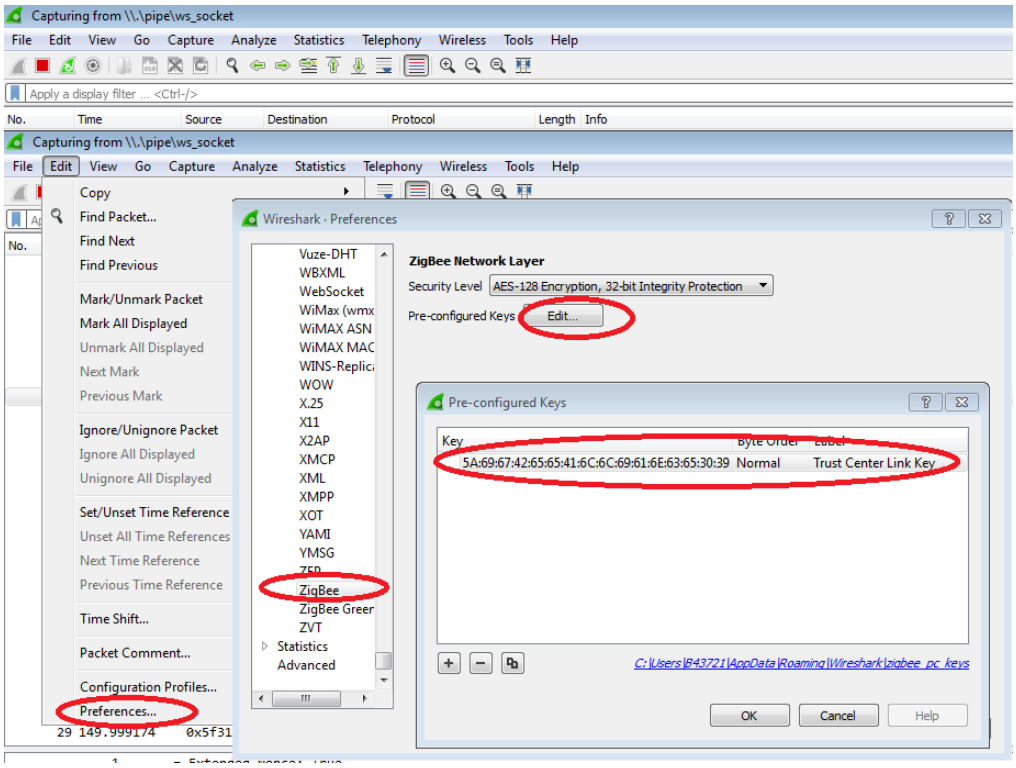
NXP 提供了 IEEE802.15.4 数据包嗅探器的 Firmware 固件。请将 JN-SW-4168 自带的 JefficSniffer 固件烧录到 JN5169 USB Dongle 中。





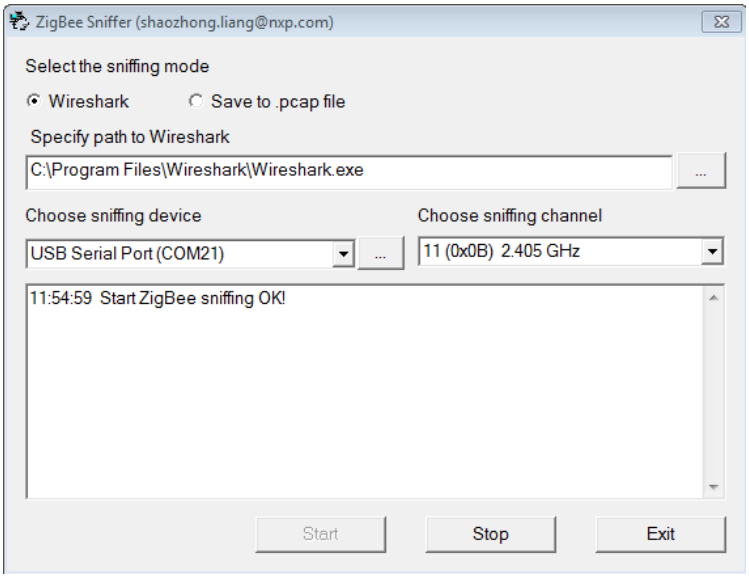
2. 下载、安装最新的 Wireshark 软件。

Wireshark 是世界上最流行的网络分析工具。这个强大的工具可以捕捉网络中的数据，并为用户提供关于网络和上层协议的各种信息。在 Wireshark 中配置 ZigBee 默认的 Link Key，否则无法解析加密网络内容。通过”Edit-->Preferences-->Protocols-->ZigBee”菜单配置 16 字节的 Trust Center Link Key={5A:69:67:42:65:65:41:6C:6C:69:61:6E:63:65:30:39}

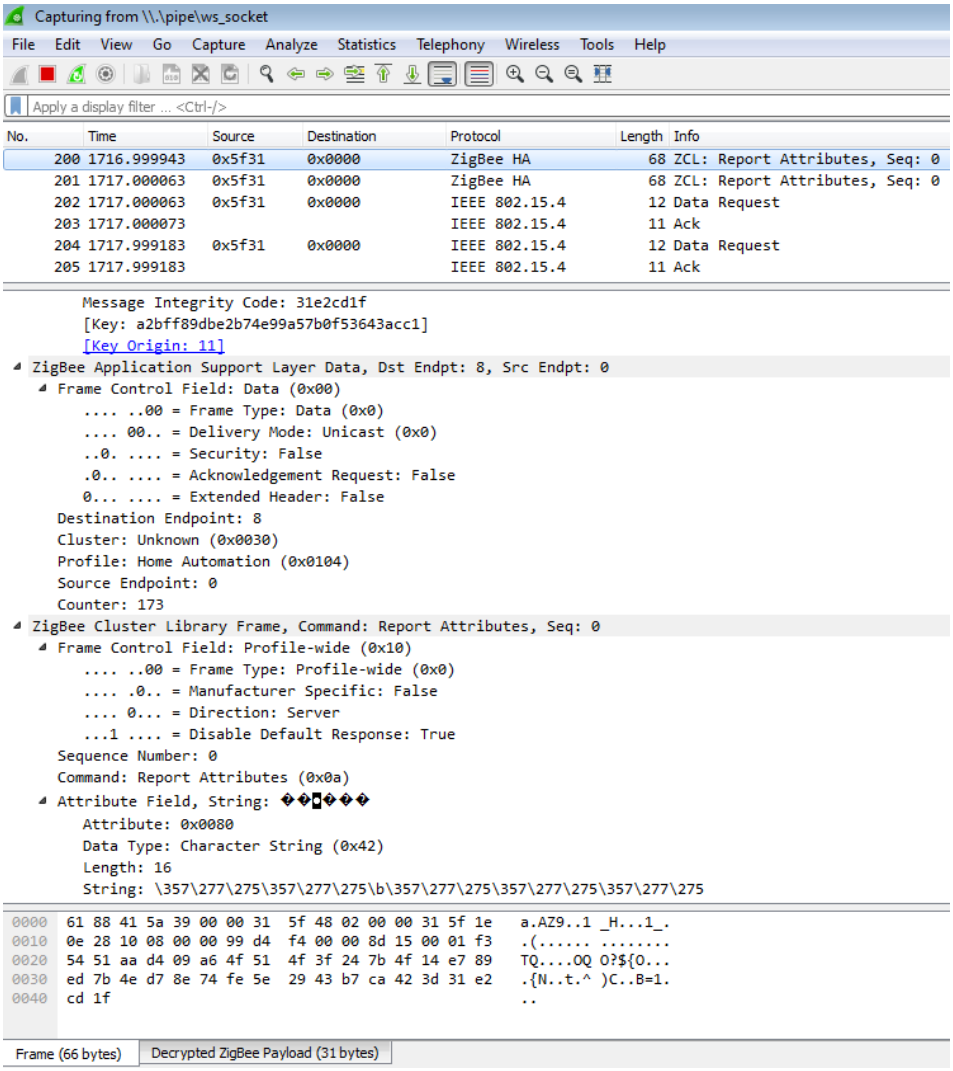


3. 在 PC 运行 ZBSniffer.exe 抓包工具

在启动抓包前，先设置 Wireshark.exe 的目录，USB Dongle 的串口端口号和 ZigBee 的运行信道。点击 ZBSniffer.exe 的”Start”按钮后启动 Wireshark。二者通过命名管道的方式交换抓包数据。Wireshark 将会接收命名管道的数据，并解析 IEEE802.15.4 数据包。



下面是通过 Wireshark 解析 ZigBee 数据包的截图，可以将 ZigBee 的各个字段进行详细解析。



4. 抓取分析 IEEE802.15.4/Thread 协议

由于 Thread 与 ZigBee 都是基于 IEEE802.15.4 MAC，所以这个工具也可以通过 Wireshark 解析 Thread 协议。