[pdctf]BTLE wp

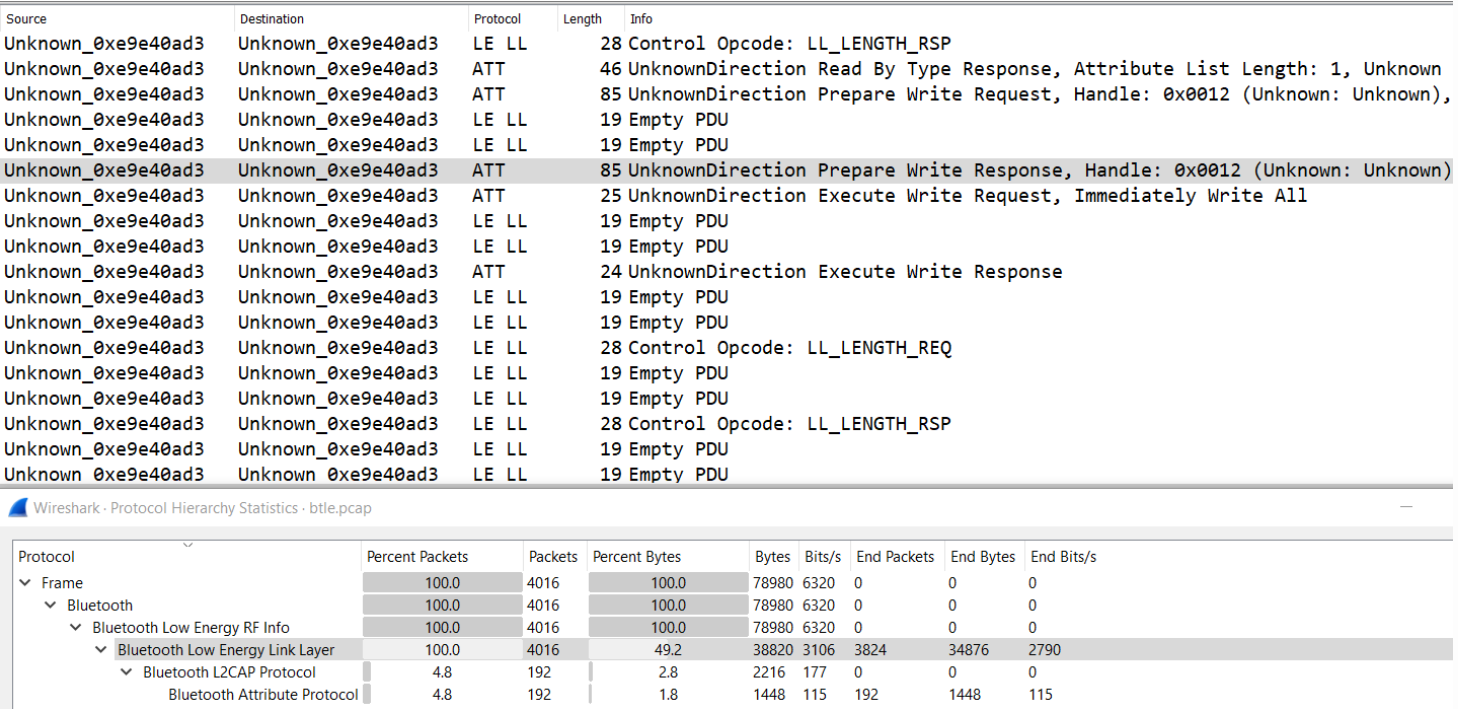
原文地址：https://www.cnblogs.com/bamboo1111/p/15401402.html

“”我将我的标志存储在远程数据库中，但是当我试图读回它时，它已被编辑！你能恢复我写的东西吗？

添加一名作者

附：btle.pcap “”

在中打开捕获文件 wireshark，我们注意到大部分数据包只是来自蓝牙低功耗链路层 ( LE LL) 的空 PDU 。



蓝牙属性协议 ( ATT) 的数据包看起来更有趣，因为它们似乎包含读/写请求，这应该是指从挑战描述中所述的远程数据库中存储和检索标志。

如果我们过滤btatt并滚动到底部，我们可以在 Value 属性中发现一个包含已编辑标志的读取响应数据包。