B.3　分析一个神秘的数据包

在图 B-2 中，我们看到了一个被部分解析的数据包。我们通过被解析的部分数据来确定，这是一个 TCP/IP 数据包，该数据包在同一网络内的两个设备间传输，然而除此之外，我们对该数据的其他信息并不了解。以下是这个数据包的完整十六进制数据：

```
   4500 0034 8bfd 4000 8006 1068 c0a8 6e83
c0a8 6e8a 081a 01f6 41d2 eac6 e115 3ace
5018 fcc6 0032 0000 00d1 0000 0006 0103
0001 0001
```

数据包大小为 52 字节。IP 协议的数据包结构图告诉我们，IP 协议头的标准长度为 20 字节；根据 0x00 字节的低位字节表示的头文件长度，我们确认了这一信息。根据 TCP 的包结构图，我们同样了解到，在没有附加选项的情况下，TCP 协议头的长度也是 20 字节（此处没有列出 TCP 结构图，但是我们在第 6 章中对 TCP 选项进行了深入讨论）。这意味着，数据包的前 40 个字节是 TCP 和 IP 协议头数据，这些数据已经被解析。现在，还剩下 12 字节未被解析。

```
   00d1 0000 0006 0103 0001 0001
```

如果没有分析数据包结构的知识，你现在可能会一筹莫展，但是你已经知道了如何将数据包结构图应用于未解析数据。在本例中，已经解析的 TCP 数据包表明，数据的目的端口号是 502。在识别未解析数据时，查看通信使用的端口并不一定会奏效，但这是一个好的切入点。Google 搜索结果显示，502 端口是基于 TCP 的 Modbus 协议的常用端口，该协议用于工业控制系统（ICS）网络。我们将十六进制包数据与 Modbus 数据包结构图进行比较，来核实和分析本例的数据包，如图 B-5 所示。

基于TCP的Modbus					
偏移位	八位组	0	1	2	3
八位组	位	0–7	8–15	16–23	24–31
0	0	事件标识		协议标识	
4	32	长度		单元标识	功能码
8+	64+	编码			

图 B-5　基于 TCP 的 Modbus 的数据包结构图

这个数据包结构图根据 Modbus 的应用指导文档制作。图 B-5 结构图表明，位于 0x04:2（相对头部起始位置的偏移量）的长度字段包含一个 7 字节的头部。按照这个偏移量，我们在对应的位置上发现其十六进制值为

0006（对应的十进制值为 6），这表明，紧随这个字段之后有 6 字节，实际也是如此。看起来这的确是基于 TCP 的 Modbus 数据。

将完整的十六进制数据和 Modbus 结构图比较，以下是提取出的信息。

- 事件标识字段位于 0x00:2 字节 （0x00～0x01），十六进制值为 00d1。该字段用于将应答和请求进行配对。
- 协议标识字段位于 0x02:2 字节 （0x02～0x03），十六进制值为 0000。这表明协议为 Modbus。
- 长度字段位于 0x04:2 字节 （0x04～0x05），十六进制值为 0006。这定义了数据部分长度。
- 单元标识字段位于 0x06 字节，十六进制值为 01。表示此数据包用于系统内路由。
- 功能码字段位于 0x07 字段，十六进制值为 03。这表示调用读取保持寄存器（Read Holding Registers）功能，用于从一个系统读取一个数值。
- 根据功能码 3，需要再输入两个数据字段。在 0x08:4 字节发现了参考编号（Reference Number）和单词计数（Word Count），这两个字段的十六进制值均为 0001。

这个神秘的数据包能够按照 Modbus 协议的标准被完全解读。如果你正在对产生这个数据包的系统进行故障处理，以上解析出来的内容应该是你向前推进所需要的信息。就算你不会遇到 Modbus 数据，对于如何使用包结构图处理一个未知的协议和未被解析的数据包，这也是一个很好例子。

了解你正在分析的数据的抽象方式，总是一种最好的分析思路。这能帮助你做出更合理和明智的决定，使你能在更多样化的场景中处理数据包。在很多情景下，我只能使用命令行工具，如 Tcpdump，进行数据包分析。因为大部分这样的工具缺少很多应用层协议的分析器，所以手动对数据包中的原始数据进行分析的能力极其重要。

> 注意
>
> 我的一位同事曾经负责在一个高安全级别的环境中进行应急响应。他很清楚他需要检查所负责系统的数据，但是不能接入存储这些数据的特定系统。在他们的工作时间内，他们能做的只有将数据包从特定的会话中打印出来。幸亏掌握了数据包组成和数据包结构分析的基础知识，他能够从打印出的数据中获得他需要的信息。当然，这个分析过程相当缓慢。这是一个极端的场景，但是，这是能证明通用的、与工具无关的知识很重要的例子。

由于以上陈述的原因，花费时间将数据包拆分，以获得使用多种方式分析数据包的经验，对我们很有帮助。我在这方面下了很多功夫：我打印了一些常用协议的数据包结构图并进行封塑，然后将这些图片放在书桌旁。我还

在笔记本电脑和平板中保存了电子版本，以便外出时快速查阅。为了方便获取，我在随本书发放的抓包文件的压缩包中包含了一些常用的数据包结构图。