5.4 协议解析

Wireshark 最大的优势就是对上千种协议解析的支持。Wireshark 有这种能力的原因是它是开源软件，能够给开发者一个创造*协议解析器*（protocol dissectors）的框架。Wireshark 中的协议解析器允许你将数据包拆分成多个协议区段以便分析。举例来说，Wireshark 的 ICMP 协议解析器可能将网络上的原始数据提取出来，对其进行格式化并以 ICMP 数据包格式显示出来。

你可以将解析器看作是一个网络原始数据流和 Wireshark 程序之间的翻译器。如果需要 Wireshark 支持某一个协议，那么它就必须拥有一个内置的解析器（或者你可以自己写一个）。